**2017年6月13日，微软官方发布编号为CVE-2017-8464的漏洞公告，官方介绍Windows系统在解析快捷方式时存在远程执行任意代码的高危漏洞，黑客可以通过U盘、网络共享等途径触发漏洞，完全控制用户系统，安全风险高危   
具体详情如下:**

**漏洞编号:**    
**CVE-2017-8464**   
**漏洞名称:**    
**Microsoft Windows LNK 远程代码执行漏洞**   
**官方评级:**   
**高危**   
**漏洞描述:**   
**攻击者可以向用户呈现包含恶意的.LNK文件和相关联的恶意二进制文件的可移动驱动器或远程共享。 当用户在Windows资源管理器或解析.LNK文件的任何其他应用程序中打开此驱动器（或远程共享）时，恶意二进制程序将在目标系统上执行攻击者选择的代码，成功利用此漏洞的攻击者可以获得与本地用户相同的用户权限。   
注释:.LNK是windows系统内应用程序快捷方式文件的文件类型后缀名。**   
**漏洞利用条件和方式:**    
**远程利用**   
**漏洞影响范围:**    
**桌面系统**

* Microsoft Windows 10 Version 1607 for 32-bit Systems
* Microsoft Windows 10 Version 1607 for x64-based Systems
* Microsoft Windows 10 for 32-bit Systems
* Microsoft Windows 10 for x64-based Systems
* Microsoft Windows 10 version 1511 for 32-bit Systems
* Microsoft Windows 10 version 1511 for x64-based Systems
* Microsoft Windows 10 version 1703 for 32-bit Systems
* Microsoft Windows 10 version 1703 for x64-based Systems
* Microsoft Windows 7 for 32-bit Systems SP1
* Microsoft Windows 7 for x64-based Systems SP1
* Microsoft Windows 8.1 for 32-bit Systems
* Microsoft Windows 8.1 for x64-based Systems
* Microsoft Windows RT 8.1

**服务器系统**

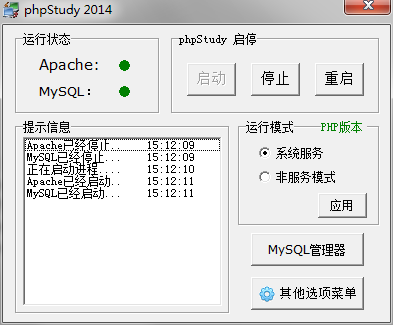
* Microsoft Windows Server 2008 R2 for Itanium-based Systems SP1
* Microsoft Windows Server 2008 R2 for x64-based Systems SP1
* Microsoft Windows Server 2008 for 32-bit Systems SP2
* Microsoft Windows Server 2008 for Itanium-based Systems SP2
* Microsoft Windows Server 2008 for x64-based Systems SP2
* Microsoft Windows Server 2012
* Microsoft Windows Server 2012 R2
* Microsoft Windows Server 2016

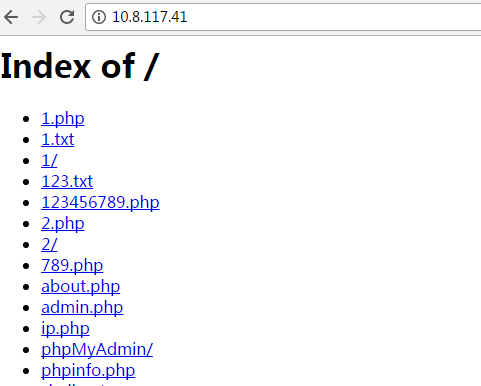
**漏洞还原:**

**利用原理：创建恶意快捷方式，包含恶意执行脚本，点击恶意快捷方式，导致本机中病毒。**

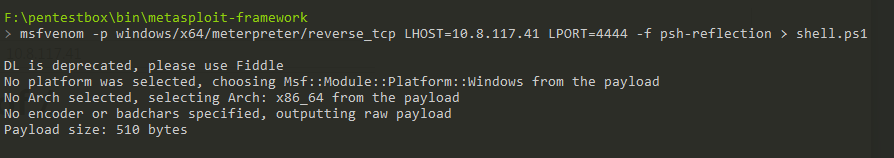
**一：本机搭建一个网站然后把恶意脚本放入网站目录**

1. **我本机演示使用的是phpstudy集成环境搭建的一个本地网站**

****



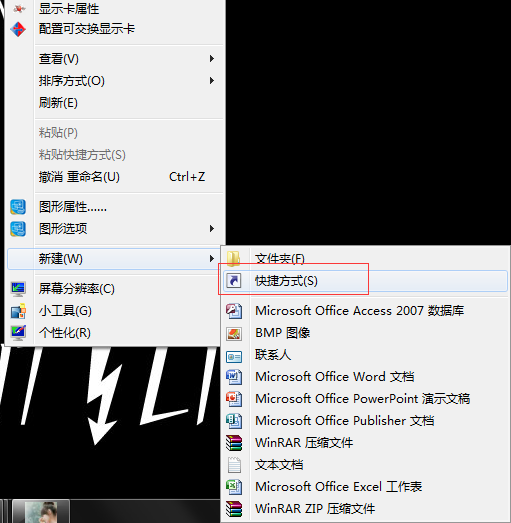
**二：利用msfvenom生成一个msf反弹后门shell.ps1，把shell.ps1放入我们搭建的网站根目录**

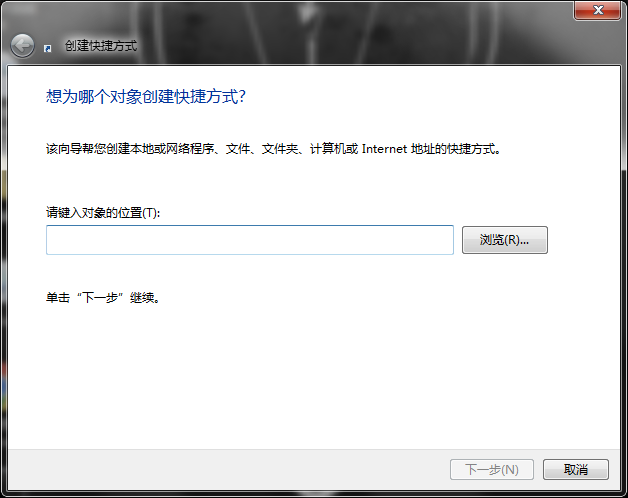




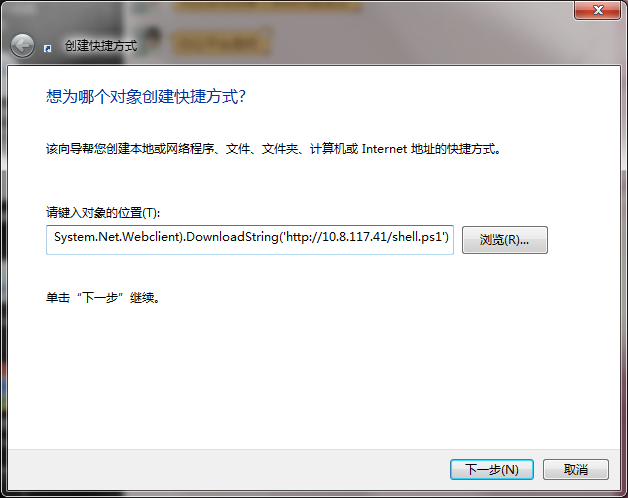
**三：创建一个恶意的powershell快捷方式**

**桌面——右键——新建——快捷方式**

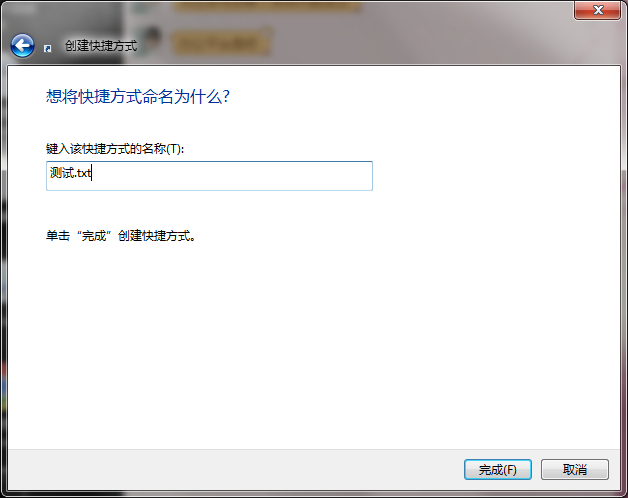




**四：在键入对象的位置放入我们的恶意远程的powershell脚本**

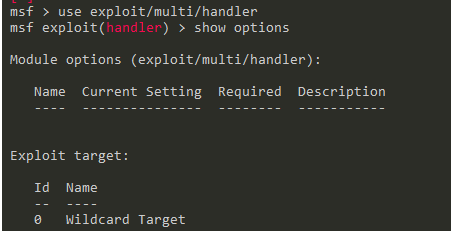


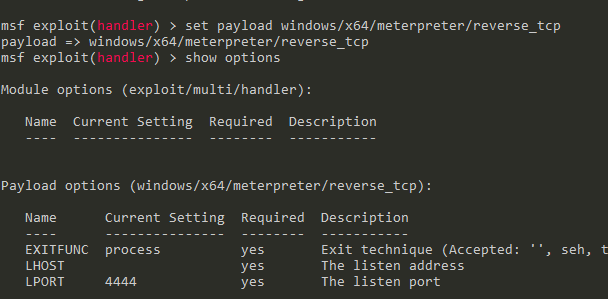
**下一步**



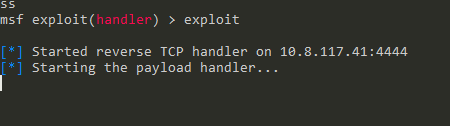
**完成**

**五：使用metasploit监听模块监听我们的木马脚本**



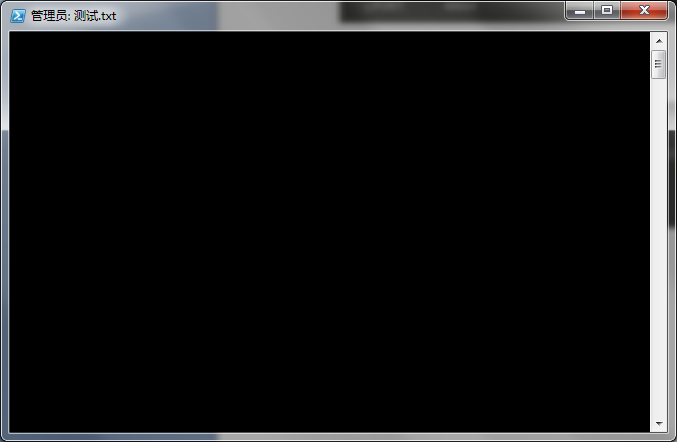


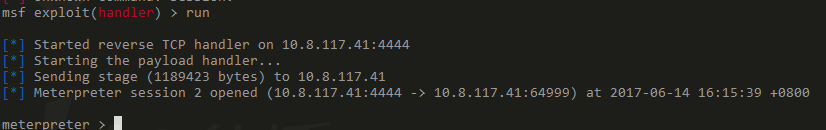
**配置好payload之后开始监听**

****

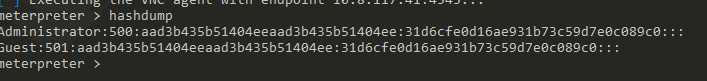
**打开我们刚刚创建的快捷方式**

****

****

****

**Metasploit成功弹回了会话**

****

**接下来 可以控制这台电脑。**

**全程下来杀毒软件没报毒也没提示。。。。。。。**

****