# 背景

网上看到的iis6.0（cve-2017-7269）的利用文章，要么只有远程利用不包含本地提权，要么包含本地提权却没有常见失败原因，故有此文

本篇文章面向有一点windows命令行基础，kali基础，msf基础的同学

# 实验环境

被攻击系统：03\_ent\_x86\_zh-chs + iis的webdav功能

攻击系统：kali2019\_x64\_en-us

先决条件：iis默认不开启webdav功能，所以需要手动开启webdav功能

# 被攻击系统环境搭建

开启WebDAV服务：开始-》控制面板-》管理工具-》internet信息服务管理器-》web服务扩展-》开启WebDAV，如下图



# 攻击系统环境准备

0：先更新系统，执行命令如下：

apt-get update && apt-get upgrade

kali下更新系统会自动更新msf

1：更新完msfconsole，通过测试发现，msf自带的这个漏洞的利用（exploit/windows/iis/iis\_webdav\_scstoragepathfromurl）无效，至于为什么无效，先不去深究（截止到2019/09/05，最新版msf自带的模块仍旧无效，不知道以后的msf更新会不会修复这个利用）

2：去网上寻找，发现[dmchell](https://github.com/dmchell/metasploit-framework/blob/master/modules/exploits/windows/iis/cve-2017-7269.rb)的漏洞利用脚本可用

# 远程利用过程如下

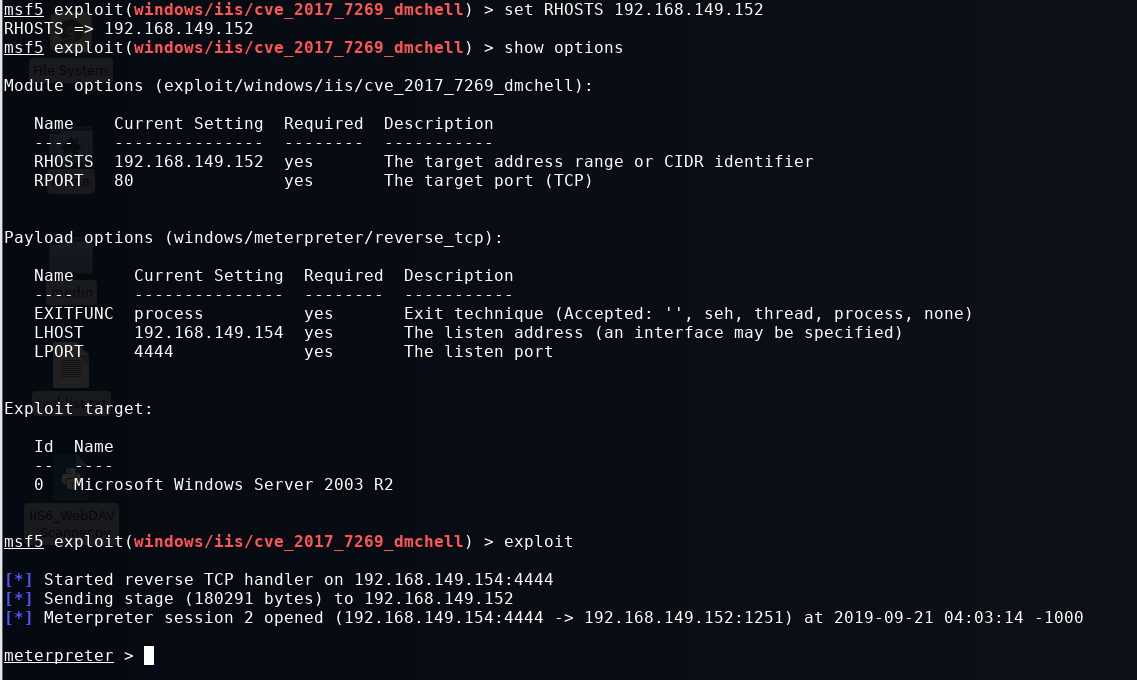
0：将ruby脚本下载下来，放到msf的模块路径下（可以放到/usr/share/metasploit-framework/modules/exploits/下或其任意子目录下），我选择放到的路径为/usr/share/metasploit-framework/modules/exploits/windows/iis/（这是kali下的msf路径，至于其他系统的msf路径，请自行查找）

1：重新启动msf（如果找不到脚本，可尝试执行reload\_all，并再次重启msf）

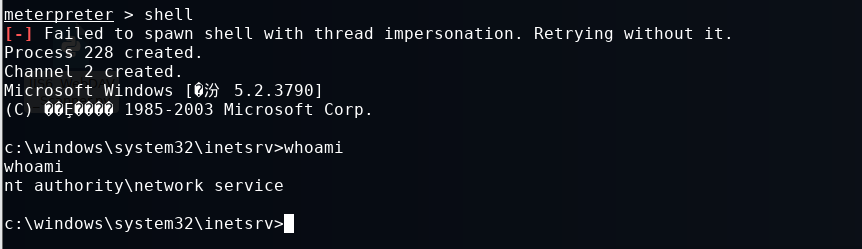
2：这个有一个坑，名称cve-2017-7269.rb会让msf载入时报错，由于msfconsole不能识别符号“-”，需将名称修改为cve\_2017\_7269.rb

3：重新启动msf，成功载入模块

4：设置参数并利用，成功拿到meterpreter，如下图



进入shell，执行命令whoami，发现权限是network service，故需要提权



# 本地提权前期准备

0：提权思路为使用一款本地溢出工具提升权限，前提需要目标没有打补丁KB952004，工具下载链接<https://pan.baidu.com/s/1MtxMIKSa2hsFiomf3JavBA>，提取码iwmy，永久有效

（如果这个补丁被打上了，还可以看看是否打上这两个补丁“KB956572 MS09-012”或者“KB970483 MS09-020 ”，这2个也常用于iis6提权，工具从网上可以找到）

1：查看系统是否安装指定的补丁，使用如下命令：

systeminfo | findstr "KB952004" # 注意区分大小写

2：后在03\_ent\_x86\_zh-chs下测试发现，不能从全部补丁中过滤，即有遗漏，改用如下命令：

wmic qfe list full | findstr "KB952004" # 注意区分大小写

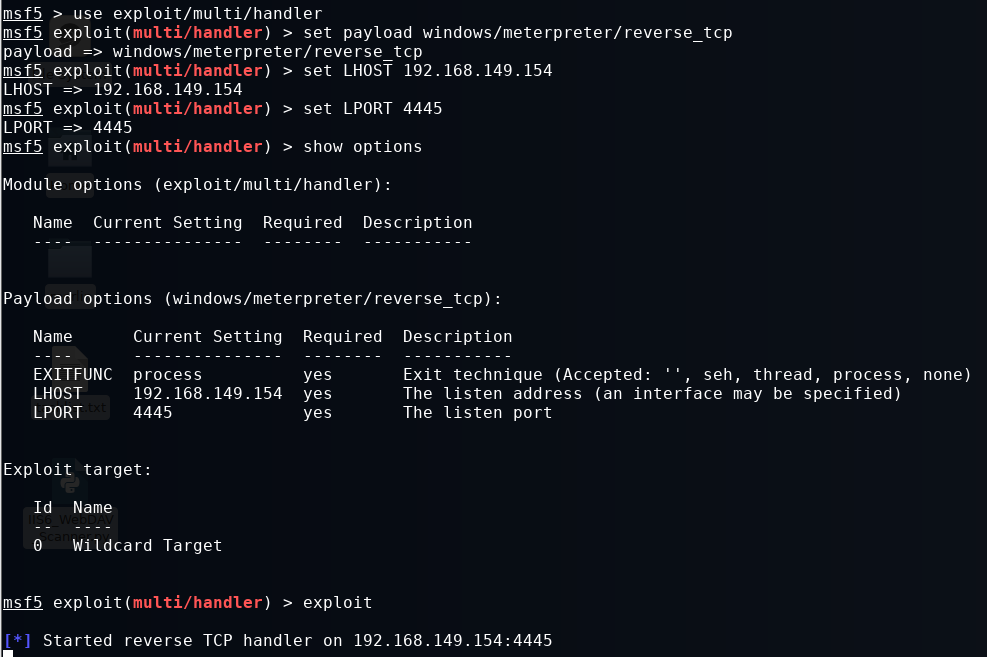
# 本地提权过程如下

0：漏洞利用后，直接上传文件会提示“access denied”， 进入系统，并在c盘下创建目录tmp，

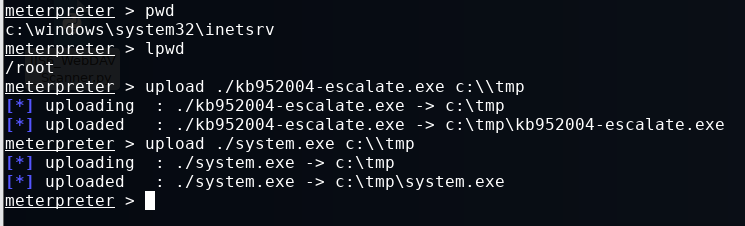
1：使用msfvenom生成payload

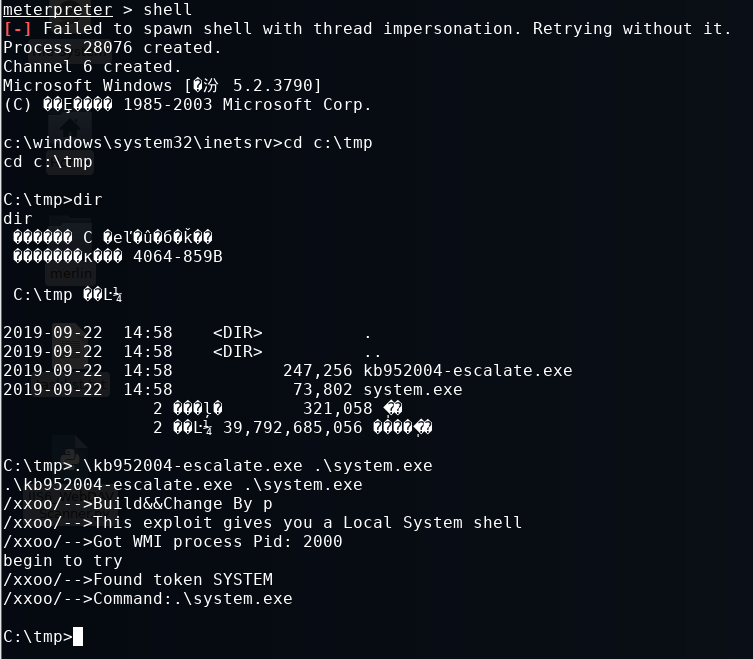


2：再开启一个msfconsole并进入监听状态

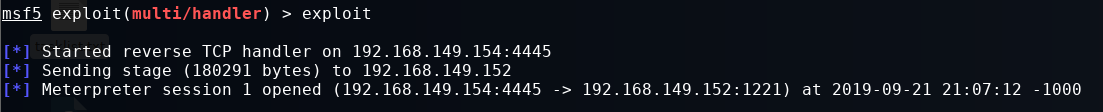


3：回到第一个meterpreter，将用于提权的程序和payload上载到目标c:\tmp下（注意，在meterpreter下，路径中带有反斜线时，需要使用2个反斜线）



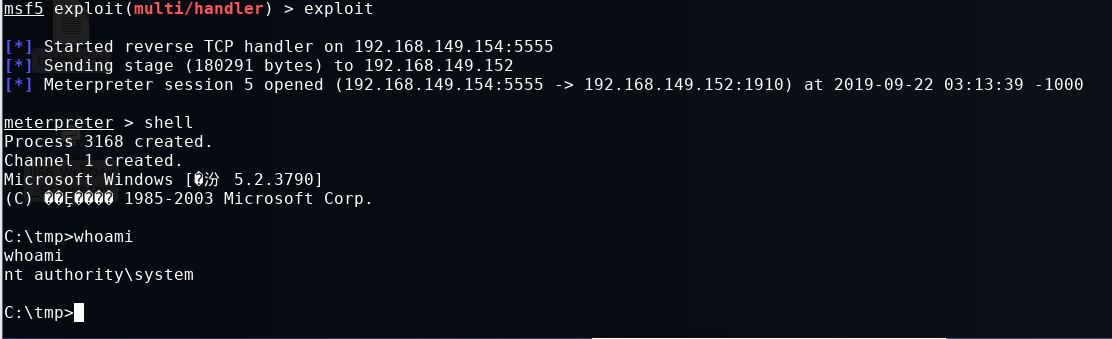
4：切换到c:\tmp下，使用提权工具执行payload

5：另一边成功拿到meterpreter（提权时有个地方需要注意，使用kb952004-escalate.exe后再回退到meterpreter时可能会导致meterpreter会话超时失效），可是会话会一直卡在这



6：后经测试发现，需将提权工具重命名为pr.exe，才能成功拿到反连shell



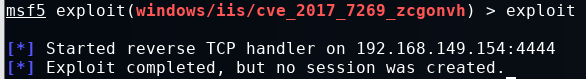


# 其它系统测试

03\_ent\_x86\_zh-chs和03\_r2\_ent\_x86\_zh-chs能被利用，即x86系统能被利用

03\_ent\_x64\_zh-chs和03\_r2\_ent\_x64\_zh-chs不能被利用，即x64系统不能被利用

如果系统打上补丁kb3197835（<https://www.catalog.update.microsoft.com/search.aspx?q=3197835>），则利用会失败，反馈如下



# 常见失败原因总结

0：端口和域名绑定问题

实际环境中，iis绑定的域名和端口可能不是默认的，所以exp中的If头信息中的两个url是要求和站点绑定相匹配的，否则只能收到一个502。这里所说的相匹配指的是if头中url的port必须与站点绑定的端口相匹配，而if头中的域名只需要和host头保持一致就好。（这里的域名需要和host头保持一致，我个人理解可能是针对CDN的情况下exp中的域名并不是host头中的域名）

1：物理路径

根据CVE-2017-7269 IIS6.0远程代码执行漏洞分析及Exploit中提到：POC中If头中的第一个URL会被解析成物理路径，默认情况下是C:\Inetpub\wwwroot\，在覆盖缓冲区的时候填充的字符长度要根据物理路径的长度来决定，且物理路径长度 + 填充字符的个数 = 114。POC中的是按照默认的物理路径（19位）来计算填充字符的长度的，当物理路径的长度不为19位的时候就会收到一个500。（这里物理路径长度计算方法要加上最后的\）

2：多次执行错误shellcode

多次执行错误的shellcode会覆盖很多不该覆盖的代码，从而导致正确的shellcode执行也返回500，提示信息为：“参数不正确”，也可能什么都不返回

3：exp执行成功后

当exp执行成功一段时间之后(大概十分钟到二十分钟左右，其间无论有无访问，被windbg挂起的时间不算)，再对这个站点执行exp永远不会成功，同时返回400。

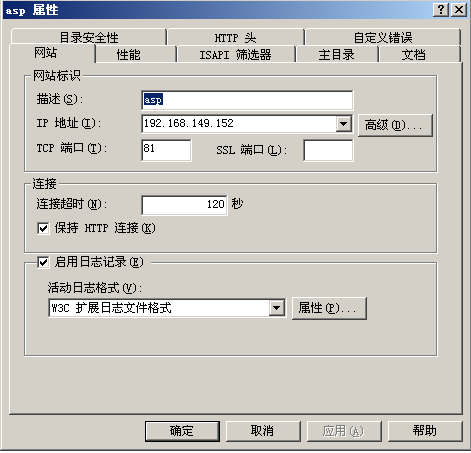
4：win03 x64

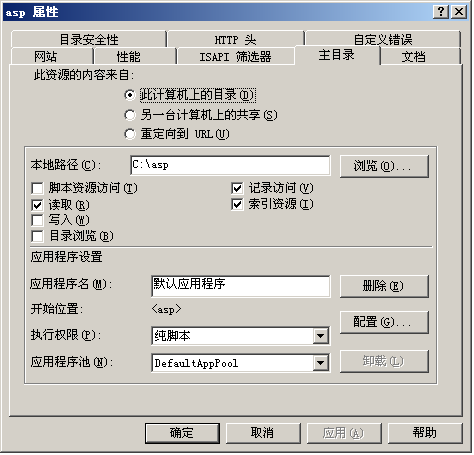
win03 x64并不多见，此类型的不能直接用网上的POC进行攻击。

# 失败原因解决方案

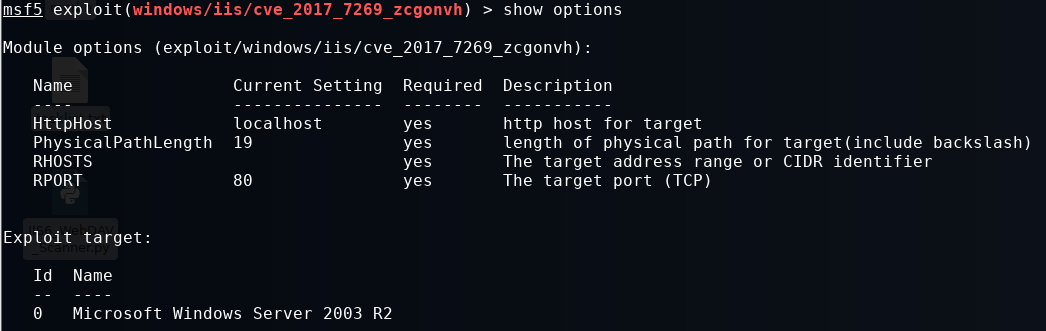
0：针对上述的失败原因，[dmchell](https://github.com/dmchell/metasploit-framework/blob/master/modules/exploits/windows/iis/cve-2017-7269.rb)的exp进行相应调整后并不能利用成功，在网上寻找，发现[zcgonvh](https://github.com/zcgonvh/cve-2017-7269)的exp在进行相应调整后，可成功利用

1：更改网站默认目这只：右键点击网站-》属性-》更改网站设置

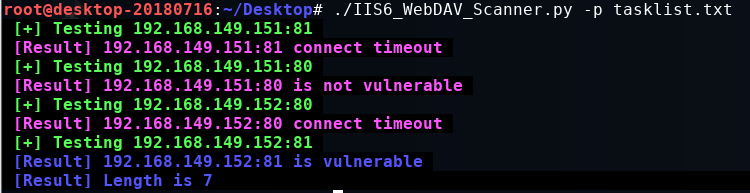




2：zcgonvh的exp的参数如下



3：其中参数PhysicalPathLength为网站路径，可以使用[admintony](https://github.com/admintony/Windows-Exploit/tree/master/IIS6_WebDAV_Scanner)的工具进行网站路径的爆破，如下为爆破结果



4：使用[zcgonvh](https://github.com/zcgonvh/cve-2017-7269)的exp，设置好参数并进行漏洞利用，成功拿到meterpreter

