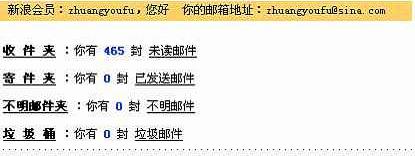
周末无聊，和眼圈聊天，告诉他我在用社会工程搞一个站点，真是没想到他竟然也在忙这个，我搞的是ARM产品的，拿到了系统管理员的密码。他竟然是在搞一个IDC公司，而且已经获得整个机房的管理员权限。看来目前的社会工程是很火的，本着发扬共享精神得原则，我们把自己的一点心得发出来，供大家参考，不足之处，还望大家多多指教。  
     渗透方式：:通过网络聊天获取对方服务器帐号密码等信息  
     渗透目标：入侵ARM产品公司，商务互联IDC公司  
     思路:客服人员信息收集(关键)---技术客服信息收集(时间简短)---机房销售信息收集(中长,自己拿捏时间)---技术人员(关键)  
     与眼圈的社会工程相比，我的是简单得多，是在了解了一部分信息后，利用欺骗得手段获得了可用信息成功猜解得到管理员密码，简要介绍一下。  
     我首先在他的站点上了解了点基本常识（啥都不知道就很容易穿帮了不是？）部分聊天记录：  
CNhCerKF 12:00:59  
     您好，请问韩永是贵公司的吗？  
     ARM产品 12:01:13  
     您是？  
     CNhCerKF 12:02:37  
     我朋友介绍的，说让我找他请教关于NK9315板子的情况的。  
     ARM产品 12:03:08  
     噢，NK9315的板子好像停产了有一段时间了   
     CNhCerKF 12:03:38  
     停产了？您是？   
     ARM产品 12:03:43我是网站技术维护，我们是做嵌入式产品代理的  
     CNhCerKF 12:04:40  
     那他是做什么的呢？我一朋友让我找他的，您能告诉我下他的联系方式吗？谢了。…………  
     ARM产品 12:07:32  
     噢，如果你需要找资料就直接告诉我吧，如果我能提供的就直接给你了   
     CNhCerKF 12:08:25  
     好的，先谢谢您了，回头我需要什么我MAIL给你。   
     ARM产品 12:08:46  
     好的，[itarm@163.com](mailto:itarm@163.com)，这是我的邮箱，给我留言也可以   
     CNhCerKF 12:09:08  
     恩。谢了先   
     ARM产品 12:09:11  
     不客气。  
     CNhCerKF 12:09:28  
     请问您贵姓？  
     ARM产品 12:09:41  
     免贵姓庄，庄有福。  
     CNhCerKF 12:09:28  
     哈，我有一哥们也叫这个名字，他是83年的，你呢？  
     ARM产品 12:10:17  
     我是80年6月11号的，比他大点。/cy  
     CNhCerKF 12:10:28  
     看来是要叫大哥了哦，顺便问下，要怎么才能直接找到你呢？  
     ARM产品 12:11:03  
     你说找100871号就可以了。  
     CNhCerKF 12:12:12  
     大哥有电话没？如果您不在线我直接TEL您。  
     ARM产品 12:13:44  
     别总是您您的，太客气了。我电话是131642778XX。  
     CNhCerKF 12:14:35  
     好的，大哥您先忙，回头找您联系。  
     呵，就这样。我得到了他的基本资料，就这样，我得到了他服务器pcanywhere以及个人的一些密码，系统管理员密码。服务器权限的丢失竟然这么容易，社会工程，取权限于无形。。  
http://forum.chinesehonker.org/images/lzdesign/attachimg.gif

http://forum.chinesehonker.org/images/attachicons/image.gif[h1.jpg](http://forum.chinesehonker.org/attachment.php?aid=2074&nothumb=yes) (14.63 KB)

2009-9-14 10:44

http://forum.chinesehonker.org/images/lzdesign/attachimg.gif

http://forum.chinesehonker.org/images/attachicons/image.gif[h2.jpg](http://forum.chinesehonker.org/attachment.php?aid=2075&nothumb=yes) (17.34 KB)

2009-9-14 10:44

     我的社会工程是最基础的，看看眼圈的吧。个人认为堪称中国的欺骗艺术，他的语气比我的要拿捏的好得多，是真正客户得风范，俺做习惯客服了^\_^  
     黑眼圈 12:47:45 您好,我想租一台主机. ……………………  
     商务互联-008 12:51:28 好的，请问你注册会员了吗   
     黑眼圈 12:53:33 是的.   
     商务互联-008 12:52:49 是多少   
     黑眼圈 12:53:54 我的Email吗?   
     商务互联-008 12:53:22 恩是的   
     黑眼圈 12:54:23 [zcboy\_3247419@sina.com](mailto:zcboy_3247419@sina.com)   
     黑眼圈 12:55:34 你怎么问我这个?   
     商务互联-008 12:55:05 我到时好给你入款啊   
     黑眼圈 12:56:14 你们提供的服务可靠吗? 黑眼圈 12:56:18 我被骗过几次   
     商务互联-008 12:55:40 是的，请放心，我们做这个行业有四年的时间   
     黑眼圈 12:56:52 今天是你接待我的.你留下你的信息.到时候被骗了,我可以投诉.   
     黑眼圈 12:57:15 把你们公司的电话地址告诉我..如果骗了我,我可以随时找你们.   
     商务互联-008 12:56:47 [www.XXinter.com](http://www.xxinter.com/) 这是我们公司的网站   
     黑眼圈 12:58:01 我知道.我看了.. 我是需要你的信息.   
     商务互联-008 12:57:13 电话是028-86086035-8xx 手机：135408415xx 王小姐   
     黑眼圈 12:58:33 王小姐?世界上这么多姓王的.我要真实姓名.如果不介意.可以给我身份证号码.到时候出了事好找你   
     商务互联-008 12:58:00 王TT 商务互联-008 12:58:55 身份证号就没必要了吧   
     黑眼圈 12:59:55 你员工号和身份证号多少..   
     商务互联-008 12:59:13 网站上都有个营业执照号   
     黑眼圈 13:00:10 我要你的员工号..   
     商务互联-008 12:59:33 你是第一个要我身份证号的客户，从来没有过   
     黑眼圈 13:00:36 不是.这不是多一个心眼吗? 我被骗了几次了   
     商务互联-008 12:59:50 这是属于我的隐私，我可以不说吗   
     黑眼圈 13:00:53 可以.但是你员工号必须告诉我.   
     商务互联-008 13:00:14 没有员工号   
     黑眼圈 13:01:29 不可能,一个公司员工没员工号?   
     商务互联-008 13:01:04 是的，我的工作QQ号就是商务互联008   
     商务互联-008 13:01:24 我所待过的公司都没有员工号  
     黑眼圈 13:03:05 身份证号码真的不能提供吗? 我只是备用不时之需   
     商务互联-008 13:02:48 51102519830215xxxx   
     黑眼圈 13:04:11 你是哪里人.什么时候出生的   
     黑眼圈 13:04:19 我已经查了身份证了   
     商务互联-008 13:03:36 你在查户口还是？   
     黑眼圈 13:05:02 不是..是你四川的吗?   
     商务互联-008 13:04:20 是 黑眼圈 13:09:03 好的.谢谢你了.我考虑下.要是决定买.明天就可以汇钱了.   
     商务互联-008 13:08:38 好的，不客气，希望能彼此信任   
     黑眼圈 13:09:37 恩.  
     如此强硬的语气，完全把她压在了下边（别想歪了啊。）获得了她的基本资料，  
     还查询到了身份证等等  
     商务互联-008的资料: 姓名:王tt 性别:女 电话:028-86086035-8xx 手机：1354084xx 出生日期：1983年02月15日 发 证 地：内江市四川省资中县 身份证:51102519830215xx  
http://forum.chinesehonker.org/images/lzdesign/attachimg.gif

http://forum.chinesehonker.org/images/attachicons/image.gif[h3.jpg](http://forum.chinesehonker.org/attachment.php?aid=2076&nothumb=yes) (30.08 KB)

2009-9-14 10:44

     开始第二步  
     技术客服  
     黑眼圈 13:14:04 您好,我是王TT介绍来的.想问下服务器技术问题   
     Wang 13:15:50 你好   
     黑眼圈 13:18:29 我想请问下你们服务器是什么地区,什么网段的.因为我本机要调试程序.   
     Wang 13:19:39 西昌电信的 222.215.152   
     黑眼圈 13:19:56 我是铁通的不会有影响吧?   
     Wang 13:20:16 所谓的影响是指？   
     黑眼圈 13:20:29 网速等一系列问题.   
     Wang 13:20:52 铁通不会慢的   
     黑眼圈 13:21:45 你随便给我个你们服务器的网站,我看下访问速度快不快   
     Wang 13:22:59 ==，我让我们IDC部门的同事加你，她比较熟悉机房那边的情况   
     黑眼圈 13:23:19 好的.打绕你了.. 你叫什么名字?   
     Wang 13:23:49 我姓王，主要处理虚拟主机问题的   
     黑眼圈 13:24:17 恩.能问你全名吗?因为我想成为你们公司的长期客户.. 所以对工作人员也应该熟悉   
     Wang 13:24:58 王林   
     黑眼圈 13:25:24 恩.好的,谢谢. 你能留个联系电话吗?私人的最好.因为网站如果出现问题,好及时联系你   
     Wang 13:26:45 86086035-8XX   
     黑眼圈 13:26:51 恩.好的谢谢...  
     这样，又获得了他的信任，和机房越来越近了^\_^  
     机房咨询  
     商务互联 13:23:32 你好 黑眼圈 13:23:39 …………………………   
     黑眼圈 13:29:06 请问远程管理FTP,我是否可以使用别的软件呢?   
     黑眼圈 13:29:35 比如说pcAnywhere等那些?   
     商务互联 13:29:57 这是技术问题 ==我问一下技术   
     黑眼圈 13:30:45 恩.好的.   
     商务互联 13:30:58IDC 机柜-2 13:30:47 可以啊 但出了问题就他们自己弄哟   
     黑眼圈 13:31:46 恩.这个是可以的.请问哪些服务器有pcAnywhere呢?我好选择主机   
     商务互联 13:33:19 服务器的标准配置 …………  
     黑眼圈 13:34:59 恩.可以的.. 不过哪些IP是开了pcAnywhere呢?我买的时候可以跟客服直接选择IP主机.这样容易管理.   
     黑眼圈 13:36:03 而且我想问下pcAnywhere的连接速度怎么样?   
     商务互联 13:36:31 这个不是很清楚 因为我们客户都没有采用 那个用起很麻烦   
     黑眼圈 13:37:55 哦.那你可以给我机房人员的QQ吗?我向他们询问一些关于连接问题的事.   
     商务互联 13:39:17 好的   
     商务互联 13:39:21 2670336XX   
     商务互联 13:39:30 你说我HTT的客户就是了   
     黑眼圈 13:40:27 请问你叫什么名字呢?   
     商务互联 13:40:48 HTT   
     商务互联 13:40:53 胡TT 黑眼圈 13:40:56 恩.好的.  
     如此的意识总是让人无奈。机房，到了。。。  
http://forum.chinesehonker.org/images/lzdesign/attachimg.gif

http://forum.chinesehonker.org/images/attachicons/image.gif[h4.jpg](http://forum.chinesehonker.org/attachment.php?aid=2077&nothumb=yes) (37.08 KB)

2009-9-14 10:44

     黑眼圈 13:43:21 我是HTT客户.想咨询服务器问题.   
     IDC 机柜-2 13:43:54 好的   
     黑眼圈 13:44:24 我想要租服务器..我想问下哪些IP有pcAnyWhere服务端   
     IDC 机柜-2 13:45:16 你是想要下载个pcAnyWhere软件吗   
     黑眼圈 13:45:43 我不喜欢用FTP软件管理自己的服务器.我比较喜欢PCANYWHERE.   
     IDC 机柜-2 13:46:08 那么说你对那个软件比较熟悉了哟 黑眼圈 13:46:22 恩.我喜欢图形界面的软件 黑眼圈 13:50:40 您怎么不说话了?  
     IDC 机柜-2 13:51:48 等哈吧  
     IDC 机柜-2 13:51:52 这哈有点忙  
     黑眼圈 13:51:56 恩.好的.   
     黑眼圈 13:58:53 您来了吗?我下午还有事.   
     IDC 机柜-2 13:59:15 恩说吧   
     黑眼圈 13:59:34 我想请问哪些服务器有pcAnywhere,而且速度怎么样.   
     IDC 机柜-2 14:05:38 222.215.1XX的服务器全部安装了 1和255除外 黑眼圈 14:07:26 那速度怎么样呢?  
     IDC 机柜-2 14:07:59 速度有100M   
     黑眼圈 14:08:19 你随便给我个IP,我去IE连下看速度IDC   
     机柜-2 14:08:27 222.215.15X.XX  
     IDC 机柜-2 14:08:37 你可以测试下速度  
     黑眼圈 14:08:36 好的,就这个了,你可以留下你的Email吗?我不常上QQ,一般用MSN  
     IDC 机柜-2 14:08:47 马云风,[mayunfeng@hotmail.com](mailto:mayunfeng@hotmail.com)  
     IDC 机柜-2 14:09:03 电话你打给销售部就行了  
     IDC 机柜-2 14:09:06 OK？   
     黑眼圈 14:09:14 恩..好的.  
     IDC 机柜-2 14:09:53 那我先忙去了  
     黑眼圈 14:09:55 恩..好的   
http://forum.chinesehonker.org/images/lzdesign/attachimg.gif

http://forum.chinesehonker.org/images/attachicons/image.gif[h5.jpg](http://forum.chinesehonker.org/attachment.php?aid=2078&nothumb=yes) (31.3 KB)

2009-9-14 10:44

     就这样，得到了机房管理人员的基本信息，就这样，猜测到了密码[mayunfeng@hotmail.com](mailto:mayunfeng@hotmail.com)，管理员到手，通过渗透整个机房接近了。。。社会工程学想想都让人害怕。希望能给各位提醒下，注意自己的安全，也不要用此对他人进行恶意攻击。我们已经通知了管理员，对于其他人所做的任何测试与S.C.T小组无关。  
  
     渗透过程:应当对客服所说的话适量的怀疑,这样可以使整个渗透过程不会出以外的差错.利用了人类的敏感思维.然后把收集到的信息,充分的在每一个能用到的细节使用.比如说收集对方Email,姓名,职务,员工号,联系电话,身份证等敏感信息.得到适量的信息就应该进一步的换目标,如果总是纠缠一个人,容易引起对方的怀疑,以及厌倦.