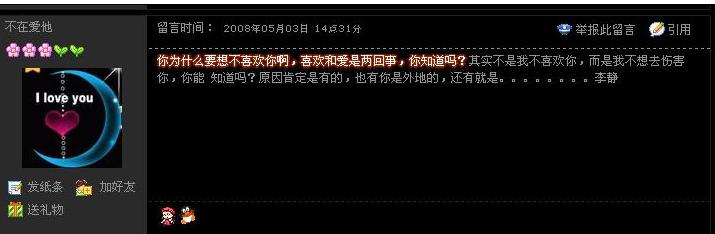
作者：菲  
                        <社会工程学的简单运用>  
  最近在研究社工,今天就用纯社会工程学盗个QQ，教大家一些用社工的一些小技巧。大致步骤。1.搜集目标资料2分析当前环境  
3.取得对方信任搞顶密码,随便找个QQ。  
                                        搜集目标资料  
  我们要开始了,现在开始搜集目标QQ资料，我的习惯是先到QQ空间找他个人资料。找不到有价值的东西在转移目标,在到别的地方找目标资料  
在QQ空间那总是会有惊喜出现,如果在空间没有找到有用的资料,不妨试试搜索网站,只要细心不怕找不到目标资料。这次也没有让  
我失望  
  
,如图1 http://forum.chinesehonker.org/images/lzdesign/attachimg.gif

http://forum.chinesehonker.org/images/attachicons/image.gif[是是.jpg](http://forum.chinesehonker.org/attachment.php?aid=2619&nothumb=yes) (24.32 KB)

2009-11-17 21:41

中可以看出目标QQ在追求留言者,也从图1中知道了留言者的名字,这对我们在搞到他QQ密码是很重要的，然后我们找到  
留言者的QQ,看看留言者的QQ昵称是什么,我用我的小号,把自己的 小号改成留言者的昵称,大家可不要只该昵称,个人资料什么  
的都要该成和留言者一样哦,  
  
如果你是黄钻用户还可以把自己的QQ空间克隆成和留言者的的QQ空间一模一样,如果不是黄钻用户克隆成的空间会和留言者的空间  
有些不一样,具体怎么克隆我就不说了,不是本文重点,资料我们就先搜集到这

分析当前环境  
  现在我们分析下环境,目标QQ是在用手机在上QQ,所以我们不用去考虑备注的问题.因为手机上是显示不出来的 的.估计目标不会记得留言者  
的QQ号.下面证实了我的推测是对的.  
                                                   取得对方信任和用社工攻击  
  做好了搜集资料和环境分析的工作,下面就是取得目标QQ的信任.然后搞定他的QQ密码,现在我们就加目标QQ,很顺利的加上了,我再利用  
已知的信息取得了目标QQ的信任。然后谎称想用下他QQ踩踩空间,开始他不肯跟我密码，我们知道目标在追留言者 。所以我们就要好好利用这一点,于是我就目标说了一句“你根本就不喜欢我 ”大家换位思考下。如果你喜欢的人和你说那样的话你会有什么反应  
呵呵...就这样轻易的搞到了 密码。下面是我和 目标QQ的对话如图2. http://forum.chinesehonker.org/images/lzdesign/attachimg.gif

http://forum.chinesehonker.org/images/attachicons/image.gif[生生世世.jpg](http://forum.chinesehonker.org/attachment.php?aid=2620&nothumb=yes) (66.87 KB)

2009-11-17 21:41

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

http://forum.chinesehonker.org/images/attachicons/image.gif[少时诵诗书.jpg](http://forum.chinesehonker.org/attachment.php?aid=2621&nothumb=yes) (80.08 KB)

2009-11-17 21:41

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

http://forum.chinesehonker.org/images/attachicons/image.gif[打扫打扫打扫大.jpg](http://forum.chinesehonker.org/attachment.php?aid=2622&nothumb=yes) (76.89 KB)

2009-11-17 21:41

是聊天记录.密码已经告诉我们了.看对不对.上去了如图9, http://forum.chinesehonker.org/images/lzdesign/attachimg.gif

http://forum.chinesehonker.org/images/attachicons/image.gif[是打算打算打打萨达.jpg](http://forum.chinesehonker.org/attachment.php?aid=2623&nothumb=yes) (134.19 KB)

2009-11-17 21:41

呵呵很简单把。文章中的不足希望大家提出来到论坛找我

总结  
  整个过程看似简单.但是有很多我的经验在里面。当你在入侵的时候可能服务器本身不存在漏洞,那你就赶快用用社工把