没有电脑的入侵－深入浅出社会工程学（part 1-3)   
  
  
作者： gouy2k & Jokul　来自：([www.s8s8.net](http://www.s8s8.net/))   
警告：请不要使用本文重涉及的任何方法进行认行违法行为    
  
基础知识    
  
在讲正题前先了解一下基本的知识吧：一些恶意入侵系统并进行摧毁的人叫cracker, 而一些只会使用别人开发的工具去入侵的叫做script kiddies. 我想这些都是大家知道的吧。 真正的黑客是具有编程能力并可以自己开发工具并有共享精神的人。一个真正的黑客不但是技术上的能人，同时，也应该是心理战术和与人交流的高手。对于怎么才能成为一个真正黑客的文章大家应该看的不少了吧，这里就不废话介绍。    
  
在这篇文章里，我并不要告诉大家怎么去用所谓的技术―包括编程或者其他网络技术去对系统进行物理入侵。我要讲的是在一种更高的技巧，就是所谓的社会工程学（Social Engineering）。 可能大家对社会工程学这个名次并不算太了解，现在我就要通过这篇文章让大家理解社会工程学是如何应用在系统入侵和应该怎么进行基本的防范。    
  
什么是社会工程学    
Social Engineering is an academic field of study to construct a theory to resolve various social problems by means of physical, social and institutional approach with special emphasis on step by step or piecemeal improvements based upon the two directional planning and designing experiences of the reality.    
  
哈哈，看不懂了吧，这是社会工程学的基本意思，上面那段话的大意是： 社会工程学是关于建立理论通过自然的，社会的和制度上的途径并特别强调根据现实的双向计划和设计经验来一步接一步的解决各种社会问题。 是不是很难明白啊。我也觉得。不用理这个，让我们看看社会工程学在我们的领域怎么解释：    
  
社会工程学是一种攻击行为， 攻击者利用人际关系的互动性所发出的攻击：通常攻击者如果没有办法通过物理入侵的办法直接取得所需要的资料时，就会通过电子邮件或者电话对所需要的资料进行骗取，再利用这些资料获取主机的权限以达到其本身的目的。    
  
现在理解了吗？？？ 如果还是不能理解我们就列举1个最最简单的例子说明一下好了：    
  
盗取qq大家知道吧，除了本地和远程盗窃密码外，还有一种方式相信大家一定知道，就是通过和对方聊天。呵呵，还没想到？？？ 你总听说过有人通过了解对方的资料来窃取qq的吧，比如说生日，姓名等等。如果有个你在qq上新加的好友，你又不熟悉他，他又迫不及待的想知道你的一切，你就要多张个心眼了，他是否想通过了解你的资料来破解的qq或者邮箱的密码？？？    
  
上面这个例子很容易理解吧，这就是社会工程学最简单的一个例子了，也许就不够资格叫社会工程学，但是道理是一样的哦。    
  
to be continued~~~~~    
  
  
  
接下来，我会列举一些所谓社会工程学使用者经常使用的手段：    
  
首先，**熟练的社会工程学使用者都擅长进行信息收集**，很多表面上看起来一点用都没有的信息都会被这些人利用起来进行渗透。比如说一个电话号码，一个人的名字。后者工作ID的号码，都可能被利用起来。举个例子， 比如说一个社会工程学使用者想从一间信用卡公司获取一些情报，但是又没有相关的证明证明他可以合法的从这间公司拿到这些情报。这时候，他就可以利用社会工程学，从和这间信用卡公司相关的银行收集相关的信息从而达到他的目的。比如说但这间银行需要从信用卡公司取得信息需要什么文件或者ID号码证明，又或者是经常与信用卡公司进行业务联系的职员的姓名等等。现在的很多公司为了方便和快捷，在一些服务上会采用电话服务，这样就更容易让这些攻击者有机可乘，只需提供从银行获得的相关资料，信用卡公司就会把一些敏感的信息给予攻击者。    
  
很多社会工程学攻击是很复杂的，包括了周详的计划，并且综合运用了相当的技巧。但是你也可以发现，一些熟练的社会工程学攻击者经常可以只用简单的方法达到他的目的，直接的进行询问来获得他所需要的信息常常是行之有效的。举个例子，某人打电话给电话公司说因为一起火灾的影响，使得附近以电话线路终端毁坏，令附近几十户人家的电话都无法使用，而他本人是个电话线路维修工，也许他可以先帮忙修理。但是修理必须需要一些电话公司不会让非本公司相关职员知道的铭感信息。但是谁又能拒绝一个好心的电话线路维修工人的无私的援助呢，这样，这位社会工程学攻击者就获得他所需要的电话线路信息。    
  
  
  
**建立信任也是一项社会工程学的手段**，**而且是相当重要手段，**试想一下如果你和某公司活人建立相当牢固的信任关系，要取得一些重要的敏感信息不就要相对容易的多了吗。要在短时间内获得信任是不容易的，但是也不是没有可能的，如果能被证明你是可以被信任的，那不就比较容易获得信任了。不明白？？ 举例说明：电话公司在搞促销，只要限定一定时间的使用和约就可以一分钱获得一部最新的手机，注意，前提是一定要签订一定使用期限的移动电话网络使用和约。有位仁兄就想了，怎么能不去花钱签订电话线路使用和约而可以以一分钱拿到这个手机呢。于是他就打了一个电话给这间电话公司属下的一间分店，我们叫它位A店。他和职员对话如下：    
职员：这里是电话公司A分店，有什么能帮你    
仁兄：你好，我叫仁兄，我之前去过你们的店，我想申请一个手机服务，你们以为姓李的店员（当然是猜的）介绍了一个不错服务给我。我当时没有拿定注意，现在我决定申请那个服务了，哦～～～，那个店员叫李～～～，我不记得了，你知道吗？？？    
店员：～～～，我们店了有两个姓李的，你说男的还是女的？？？    
仁兄：对，是男的，他说他叫李～～，不好意思，我忘记了名字，你能告诉我吗？？    
店员：叫李XX    
仁兄：对，就叫李XX，我马上就去你们店里办理相关服务开通的手续。再见    
店员：再见。    
  
之后，这位仁兄又打电话给了令一间分店，分店B    
仁兄：你好，请问是分店B吗    
职员：是，请问有什么可以帮你    
仁兄：我是分店A的李XX,我这里有一个顾客刚刚和我们签订了那个一分钱手机换购合约，但是之后我才发现店里那个手机的型号已经没有存货了，你们店里还有吗？？？    
职员：有的    
仁兄：好级了，我已经和他签订了线路使用和约，我现在叫他去你那里，你用一分钱把手机卖给他就可以了。    
职员：好的，你叫他来吧。    
  
半小时候，这位仁兄出现在了分店B里，用一分钱换购走了手机。    
  
现在明白了吗？？？**只要证明自己是可以被相信的，欺骗是很容易的。**    
  
to be continued~~~   
  
到现在为止你一定会问，这和计算机入侵有什么关系啊，呵呵，看上去没有关系，但是我讲的是手段的原理。现在我们就看一位熟练的社会工程学黑客是怎么在一个内部网里面安装木马的：   
地点一：办公室A，电话响   
职员：你好，我是小王，这里是A办公室   
攻击者： 你好，我是网络技术支持的李xx, 我们正在进行正常的网络维护，请问你们办公室的网络有出现任何问题。   
职员：嗯，据我所知没有。   
攻击者：你自己在使用上有什么问题吗？   
职员：没有   
攻击者：好的，我想说的是如果网络有任何问题及时通知我们是很重要的，我的任务就是确定没个办公室的电脑可以保持在线。   
职员：我们这里的网络状况良好。   
攻击者：我所说的情况是有可能出现的。如果出现了任何情况，请你及时打这个电话告诉我们。电话号码是：12345678   
职员：好的，如果有情况我会及时通知你们的。   
攻击者：还有一件事情。你能告诉我你的电脑所连接的端口的号码吗？？   
职员：端口？？？   
攻击者：就是在你电脑后面，在插网线的地方有注明端口号码。   
职员：看到了，号码是123.   
攻击者：请稍等，端口123~~~~.好的，谢谢。记得有情况及通过电话时通知我们，再见。   
  
地点二：此公司的网络管理室，电话响   
  
网管： 你好，网管室   
攻击者：你好，我室办公室A的小王，我们的正在解决我们电脑网线上的一点问题，你可以暂时停止端口123的网络连接吗？？？   
网关：好的，请稍等～～～，好了，已经暂时停止了。   
攻击者：谢谢。   
  
一个小时之后，攻击者的电话响   
攻击者：你好，这里是网络支持，我是小王。   
职员:你好，我是办公室A 的小李，我们的网络出现了问题，我们的电脑不可以保持在线状态了。   
攻击者：嗯，我可以帮你解决，但是我现在先要解决其他办公室的网络问题，你可以等等吗。   
职员：要多久，我没学要使用网络啊   
攻击者：我会尽快的。请稍等。   
  
这样，攻击者又打了一个电话给网管室，要求网络管理员打开的办公室A的网络连接。   
  
半小时候，办公室A,电话响   
攻击者：我室网络支持的李xx   
职员A: 你好，解决了吗   
攻击者：已经好了，请你试试   
职员A：~~~~~,是的，已经可以用了，很感谢你。   
攻击者：好的，但是有一个问题，为了不让办公室电脑的网络老是和网络断开连接，我们设计了一个软件，我把地址给你，请你去下载并安装这个软件，网址是。。。。。。。   
然后，攻击者知道这个职员去到一个他实现准备好的网页，并下载了一个小软件。   
职员A: 我执行了这个软件，但是什么都没发生啊   
攻击者：嗯～～～，也许我们在编写的时候出现了一些错误。这样吧，你不要再尝试安装了，等我们重新编写后你再装吧。   
  
就这样，一个木马程序被安装到了这台电脑上面。   
  
如何，入侵者不用任何的繁琐的电脑入手段就轻易的把一个木马安装进了网络中的一台电脑，这就是社会工程学的威力了。   
  
除了上述的方式，电子邮件也是一种手段，比如说你经常会受到一些做广告用的垃圾邮件，这种邮件平常你看都不看就会删掉吧。但是别有用心的人是不会这么笨的，假设你受到这么一封邮件：   
亲爱的小王：   
附件是我答应给你介绍的漂亮女孩的照片，看看吧，有兴趣的话我就介绍给你。   
小李   
  
这种比较私人的邮件在一般情况下是不会让人有什么怀疑的吧，最多以为是一封发错地址的邮件，再加上人的好奇心，很少人不会去不打开看看到底是什么样的漂亮女孩吧。呵呵，当你点击照片的时候，你已经不知不觉的中招了。