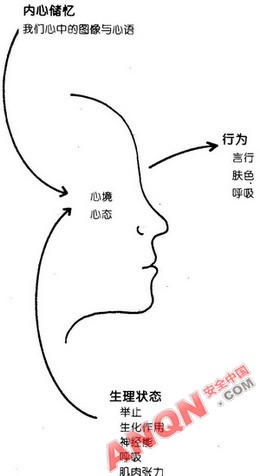
大家一定知道超级黑客凯文·米特尼克吧，深为他的社会工程学所折服，美国国防部、五角大楼、中央情报局、北美防空系统……都是他闲庭信步的地方，没有人怀疑他的真实身份，对于他所想获得的信息如鱼得水，这便是社会工程学的魅力。当然，社会工程学不是那么困难难以撑握，本文分为社会工程学—信息刺探、社会工程学—心理学的应用、社会工程学—反查技术等三部曲使大家走入社会工程学的神秘世界。 社会工程学师一般都干了什么呢?恐怕小菜们一定很想知道，是的，他们的目标或许是你的银行账户、私人信息、或是对企业拿取一份商业秘密。不管如何，他们总会设法找到一个切入点，哪怕只需要你的一个名字，他就能越过你所装的最好的防火墙或是杀毒软件，听上去有点恐怖，但事实如此，如果他们开始精心设计一个的陷阱，一切皆有可能。   
　　前言  
  
　　在前几期的<<黑客X档案>>有介绍过一些社会工程学的技巧，但是，那是狭义的社会工程学，有的是与社会工程学没有关系，比如利用dirshell扫描出大量的数据库，一旦其中存在Email与QQ，便利用其密码尝试，运气好便可成功获得真实密码，事实上这与心理学有关系，一般而言，18岁以下的人所拥有的密码为1~2个，其它为1~3个。为什么会出现这样的呢?大部分人凡事讲究方便自已，自信自已的信息一直处于安全状态。小菜们一定看到，狭义的社会工程学给人的是不可信的。广义的社会工程学是怎样的呢?说白了便是空手套白狼。它要求的是你不仅知道目标的计算机信息，且必须通过信息收集了解目标弱点，即规则弱点、人为弱点，然后开始构造精心的陷阱让目标交出攻击者所想要的信息。  
  
　　这里说明一些社会工程学的误区，有的并不能称之为社会工程学，有的小菜别被误导了。比如为了使用findpass找在线管理员的密码，而shutdown掉服务器，迫使管理员登录。请记着，这并不能称之为社会工程学，而是一种蠢方法，虽然shutdown了服务器，你能知晓管理员在线?明天或是后天，你有精力不停的等待么?菜鸟要知晓的是，社会工程学前提是离不开信息刺探，我们更好的方法是便是从筛选的信息将目标一步步引导入自已的控制范围。  
  
　　不可否认，社会工程学与生活的相关事物存在共通性，比如社交、商业、交易等都能看到社会工程学部分的影子，然而人们无法感觉。即使计算机与Internet相隔，配备高级入侵监测系统，而且也是专家人物维护，但不可忽视的是：每个人，都有弱点!而社会工程学师不但能善用这种弱点为他们服务，更危险的是，这种稍闪即逝的入侵难以察觉。这一部分简而言之使小菜明白狭义的社会工程学与广义的社会工程学的区别。下面将走进的第一部分便是信息刺探……第一部分：社会工程学—信息刺探   
  
　　一、善用你身边的信息  
  
　　尽量利用现有所知道的信息，这些信息将能处理好突发事件，此类信息指的是规章、制度、方法、约定。规章，指的是一个行业的规章，我们可以认为是行规，或是内部约定，比如，货摊A为了抢掉货摊B的生意，故意低压低价格来龚断是不对，违反了不正当经营法了。　所以我们要尽量了解各行各业的之间的此类信息，比如校园，只有领导层内的人员才会拥有一份全校的师生的联系名单，服务行业通常有这样和那样的内部约定，了解此类信息对我们非常有利。  
  
　　除了我们必须知道那些方法外，还需要的是业内术语。看到这儿，小菜一定会问什么是术语了，它主要有什么用?嗯，业内术语即不同行业之间的”黑话”，比如，我们黑客界的网络钓鱼术语，一般人会认为是到网上去钓鱼。当然，业内术语用处大着了，**社会工程学的身份都是经常变换的**，**假设我们要冒充银行业务员，就必须知道一些压缩贷款、反担保、关联企业……等等一些术语，否则当我们试图拨通一个分行经理的电话，他们就会出现激警，即经理发现你的攻击行为，由此可见术语的重要性。**  
  
　　所以在一个攻击的起始，我们得做一些准备，假设我们的目标是一个数据恢复的企业，我们可以去买一本关于数据恢复的书，熟悉一些术语的概念。顺便伪装成一个访客看看一些员工办室墙上或是桌上的规章制度，如果去他们的垃圾处理场所，总会有一堆废纸什么的，但这里面包含了重要的信息，我们可以称之为垃圾的价值，比如会有一些客户书，员工身份号联系等。现在，小菜们一定明白，任何的信息都有利用的价值。  
  
　　二、学习侦探的伪装  
  
　　假设我们获取了目标部分信息，但必须通过对话得到更加敏感的信息，我们不可能直接让对方发现吧，所以我们得先完成**身份的伪装**。假设一个小菜的目标是某电器分行的销售部，那么我们最好伪装成另一分行的销售人员，而且我们知晓他们公司内部的销售术语，或我们再带一份分行销售报告书，我想对方一定不会怀疑你不是内部人员的。  
  
　　**任何的社会工程学师都会使人认为他是可信任的，友好的，有礼貌的，然而，这都是他们伪装出来的假象。**如果要表现出文质彬彬，这会要求我们行为与语气上伪装。社会工程学师有一点比侦探更妙的地方是不需要去往自已嘴上贴胡子，哈哈。所以说，如果小菜想让MM喜欢的话，不妨去模仿她心目中的男孩。  
  
　　**再谈一下伪装的要点，任何情况不不要泄露自身的真实信息。**或许我们会碰到一些意外事件，所以，在开始准备的时候，带上一张没有多少余额的手机，用完后就别再用了，这样可免遭怀疑。还有比如通讯账号QQ，永别使用自已的QQ，最好为自已准备一个信封，目标信息拿到后，将对方拖入黑名单。  
  
　　三、人性的弱点  
  
　　**每个人都有心理弱点，没有人永远没有心理弱点。**可以说，此部分是社会工程学重要的部分，他们能够利用人们的信任、乐于助人的愿望和同情心使你上当。那么，我们应该怎样去发现这类弱点呢?很简单，我们只要构造一个精心的问题，冒称他们的同事，设计一个帮助他们解决一个问题，那么，对方便会信任我们了，我们会更轻松获得想要的信息，而且更不容被发现。菜鸟们一定经常有很多问题吧，但他们总是茫目的去找一个人帮助，或是想认一个师父，我有个这样的经验，**一个晚上我收了50个徒弟，然而只是开了一个玩笑，我的方法很简单，直接在Google搜索：本人找师父，或在qihoo搜索：找师父。然后帮助他们解决一个问题，两三句话便获取了他们的信任，有的还打算花钱请我，但我告诉他，只是开了一个玩笑，这个实例利用了他们对帮助的人信任。**此部分最具危害性，所以我进行分开来讲，请参照社会工程学--心理学应用。  
  
　　四、组织信息　构造陷阱  
  
　　假设现在我们通过目标的同事撑握了信息，比如目标的真实姓名、联系方式、作休时间…等等。这还不够的，**高明的社会工程学师会把前前后后的信息进行组织、归类、筛选。以构造精心准备的陷阱，这样，可使目标自行走入。**我打个比方吧，声明哦，这是我朋友的一个案例，  
  
　　A：你现在打不开论坛对吗?  
  
　　B：是的，打开是一片空白  
  
　　A：那是由于身份认证错误，我是XX论坛管理员，你要把论坛的用户名与密码发送到[XX@263.com](mailto:XX@263.com)，以免系统稍后会恢复你的访问。  
  
　　B：现在吗?  
  
　　A：是的，我得马上给你恢复，不然我作废账户了。  
  
不一会儿，朋友很顺利得到他在某论论的VIP账户，论坛为什么打不开了，被DDOS了，从这个例子我们可以看出组织信息的重要性，如果B能正确回答第一个问题，A可能会考虑换种方式，这个案例非常的简单，那就是B对计算机方面不了解，害怕账户丢失，一点也不怀疑A就给了密码，而这个密码已乎通用了，所以现在小菜明白前辈们总告诉你不要使用同一个密码，永别把密码告诉第三者。 　  
  
第二部分：社会工程学—心理学的应用   
  
　　从前面所说，我们知道人性的弱点在社会工程学中是重要的一部分，实际上，这是一种心理学的应用，是社会工程学的一个分支，本文从心理学角度分析社会工程学师凯文.米特尼克所著《欺骗的艺术》三个典型攻击案例，为大家揭开心理学在社会工程学中的应用。为节省篇幅，我不打算将案例拷贝过来，所以请参照光盘附带的《欺骗的艺术》文档进行阅读。  
  
　　信誉支票  
  
　　攻击者需要从国家银行查询一个用户的交易记录，然而，银行不可能答应这样的要求，所以攻击者开始他的动作。第一个电话，攻击者拨通了国家银行的电话，以私人问题顺利从吉姆.安德鲁斯获知内部专业术语。第二个电话，攻击者以信誉支票的客服代表拨通银行开户处，以调查方式获取了他想要的信息。第三个电话，攻击者以国家银行职员拨通信誉支票处，最终知道目标的用户的账户交易记录。以下标有双引号的文字，均为引用凯文.米特尼克的分析与总结。  
  
　　"我给银行打电话时，第一位年轻的小姐，吉姆，在我询问他们如何向信誉支票确定自己身份时就有所迟疑，她犹豫着，不知道是否应该告诉我"。犹豫给我们传递了一个有效的信号，可以说此时的心理想法完全在于她左脑的判断。左脑主管言语活动(听、说、读、写)、数学运算、逻辑推理等具有连续性、有序性、分析等功能，是进行抽象思维的中枢，所以这个时候我们需要给对方一个可信的理由。我想你一定有过在外借钱的经验，当你试图询问一个陌生的小姐时，她会有点儿犹豫，而如果你告诉她，你是一名导演，在外迷路了，并给她一张导演名片，我想陌生的小姐都不会拒绝，因为小姐确信他是一名导演，名片使她无从怀疑。  
  
http://forum.chinesehonker.org/images/lzdesign/attachimg.gif

http://forum.chinesehonker.org/images/attachicons/image.gif[1.jpg](http://forum.chinesehonker.org/attachment.php?aid=1691&nothumb=yes) (18.56 KB)

2009-8-17 15:09

　　"你必须依靠自己的感觉，仔细的倾听马克[受骗者]的说话内容和说话方式"。我们每个人的人生是奠基于两种形式的信息传送上。第一种是内在的传送，那是在内心里的描绘、细语和感受;第二种是外在的传送、包括言词、语气、表情、举止、行为等来与外界接触，这决定了社会工程学是否成功。**社会工程学师必须通过外在的传送来筛选最有用的信息，来判断对方的性格，感觉类型，心理特点。**各种情绪的反应过程和导演的工作很像。不错，**他们为了确实达到戏剧效果，就得掌握住观众的视觉及听觉。**如果他要你害怕，就会提高音调，并出奇不意地在银幕上跳出意想不到的画面;如果他要你兴奋，他会利用音乐、灯光，以及会有那种效果的的画面。即使是一个素材，导演也可以弄出一部喜剧或悲剧来，全看他是打算如何在银幕上呈现。如果我们要控制一个人的心智活动，产生生理的行动，我们完全可以模仿斯皮尔博格导演一样灵巧。  
  
　　**"获得公司职员认为无关紧要的信息(实际上它是有用的)"。**人人都有一种心理，那就是自已无关紧要的信息随处放着，或许，他们认为很方便。我曾住在校外时，总有一些人让我帮他们去取钱，然而，他们总把密码写在存折卡上，他们似乎认为别人没有卡就不能取钱，便如果我拿着他的身份证去挂失呢?你经常一定看到**QQ上某人的个人资料吧，通常是站点、一段数字、手机、邮件、个性签名，QQ-Zone，这给攻击者很大便利，他们会很快判断你的事业，心理弱点。**某天一个陌生人说，我与你是同一个学校(公司)，我知道你的名字，请别怀疑，快去更改你的资料吧，最好不要泄露你真实的联系方式，社会工程学师都精于此道。  
  
　　一美分的手机  
  
　　无线通讯公司发起了一个大规模的促销活动，只要你登记接受一种资费方式，便可以得到一部全新的手机，只收一美分，然而精明的人知道有很多问题要问清楚。然而攻击者讨厌捆绑资费方式，他开始行动......第一个电话拨往西吉拉德电器连锁店的泰德，谎称是顾客很顺利套取到另一职员姓名威廉.哈德利。第二个电话拨往北广街连锁店的凯蒂，冒称威廉.哈德利使凯蒂信任他是连锁店内部人员，并遵从他的要求将一美分的手机售给泰得.岩西(攻击者)。  
  
　　"人们会很自然地相信熟悉公司内部的业务流程和专业用语，并声称自己是公司同事的人"。在这一部分，我试图以心理学中的NLP神经语言学来解释，简单说NLP就是研究语言，不论是有声或是无声，对神经的影响。我们的能力是奠基于自我控制神经系统的能力，凯文.米特尼克就是透过神经系统传送特别的信息。你知道**社会工程学经常使用的技法便是冒称身份，使对方认可为内部人员。**然而以NLP来说，这种技法称之为模仿，NLP的三种形式：信念系统、心智序列、生理状态，这三种形式你并不用花过多时间理解。事实上，**NLP是强调行为、内心储忆、生理状态模仿，而社会工程学师冒称身份以及使用专业术语，那是行为上的模仿。**如果在行为的模仿无误，别人便不会对你产生丝毫怀疑，**由于公司强调的是团队与协作精神，这成为每个职员左右铭，对于同事的请求与帮助都不会怀疑其可信，否则便与公司的团队精神背道而驰，除非对方细心确认。**  
  
　　有必要单独介绍一下NLP内心储记作用，它经由五类感觉器官而测得的，换句话说，我们对周遭的认识，是透过视觉、听觉、触觉、嗅觉、味觉而传送的讯息。所传至脑子的信息就称之为感元，其中以视、听、触感元为主。不同的人感元不同，有些人觉得图画对他们会有较大诱力，另外一些人都具种感觉倾向，内心储记很少在社会工程学中利用，因为这种攻击来去匆匆以保证免遭发现，若想一个星期使人信任你，未为失一个很好的方法。很多人一定有过追女生的经验，你们一定会问她：你喜欢看电影还是听歌?或是喜欢小饰物?假设她说喜欢看电影(视觉型)，你可以夜晚放烟花，或是在一堆气球写上我爱你，那么，对方会开始对你产生信任感。你现在一定明白一些家庭不合，假设男的是听觉型，女的视觉型，女的若是问，你爱我吗?若男的说我爱你，女的说我无法感觉你爱我，很显然，他们存在信任的危机，如果男的开着车去她公司送一束鲜花，结果显而易见。  
  
　　网络故障  
  
　　鲍比的任务：对斯达伯德造船长办公室电脑进后木马植入。第一个电话，鲍比冒称服务中心艾迪.马丁，谎称网络问题的出现，并套取到计算机端口号。第二个电话，鲍比冒称鲍勃请求厂技术支持封掉端口号。第三个电话，汤姆.狄雷的求助掉入艾迪的陷阱，第四个电话，汤姆完全信任艾迪了，运行了鲍比的木马程序。  
  
"这一次由于帮他解决了问题，令对方心存感激，于是汤姆同意下载一个软件到他的计算机上"。这种心理很多人都存在，因为**我们无法质疑对方诚意的帮助，而松懈对攻击者的信任**，若不能识别这种伪造的帮助的话。正如凯文.米特尼克所说：那很令人惊讶，基于**那些精心构造的请求社会工程师可以轻易地让人们帮他做事。**前提是引起基于心理作用的自动回应，依赖于当他们觉得这个打电话的人是盟友时人们心理的捷径。人们建立信任有多种途径，然而他们都是无恶意的有意或是无意地通过交谈与帮助建立信任关系。可社会工程师才不这样想，他可以调查你暂时遇到哪些问题?如果你不经意在论坛或Google讨论组进行求助，他会很轻松帮你解决，否则他可以自行给你制造问题，以期建立信任关系。**对于伪帮助式的攻击，我们中国人或是大部人心理都存在这样的弱点，人是善良的，不可能时刻对攻击者保持警惕性，除非个人进行细心验证。** 　  
  
第三部分：社会工程学—反查技术   
  
　　什么是反查技术?即反侦查技术。在黑客攻击中，最重要的一部分不是成功侵入主机，而是清除痕迹，不要让管理者发现被侵入及数据被伪造。同理，社会工程学也有这样的概念，那么，我们得清除哪些痕迹以免遭网络0察(以下称之为网警)的发现?这一部分我们从网警角度来看问题，看看他们如何来能否找到社会工程师的蛛丝马迹。或者一句玩笑话：他们无法那么轻松找到一点痕迹。这里我们以案例来讲解，请注意，这是虚拟案例，不当之处，敬请指正。  
  
　　现场  
  
　　<<谁动了企业的数据?>>　数据存储服务部　小张  
  
　　小张正忙着登记取出数据的客户，这时内线突然响起。  
  
　　小张：你好，数据存储服务部。  
  
　　小王：我是数据存储后期服务部小王，我们前台计算机出现故障，呃，我需要你们的需助。  
  
　　小张：我可以知道你的员工ID吗?  
  
　　小王：嗯，ID是97845。  
  
　　小张：我能帮助你什么?  
  
　　小王：我们网络出现故障，我需要你把XX企业数据复印一份，然后放在二楼客户接待柜台，我们的人会取的。  
  
　　小张：好的，现在身旁还有一大批的事，我马上给你送去。  
  
　　一如攻击者所想，他很如愿拿到某企业内部数据，并将其公布到网上。这使该企业受到严重经济损失，他们开始向网警报案。然而，没有一切线索，电话是企业的内线，而那个所谓的小王根本不存在，数据存储服务器更是完好无损，迫不得已，他们开始设法从网上流传的企业数据追查IP来源，然而数据是经过多重路由传输，且经过了加密，案件陷入了绝境。相信小菜们一定有三个疑点：1.攻击者如何知道内线号码?2.攻击者为何有某员工ID?3.攻击者使用什么方法隐藏了IP?这很简单，如果你去医院看过病，一定会注意墙上的主治医师名单，上面标有ID，联系方式，及所在楼层房号，医院的目的在于更佳完善为患者提供服务。同样，数据存储公司也设了这样的名单。然而，这个案例里的小王没有进入数据存储服务公司，而是付了一部分费用给垃圾处理公司，允许他从中寻找一些东西，而攻击者寻找的是一份旧的员工联系名单，旁边也附了内线号码。  
  
　　IP如何隐藏的呢?我们看看四种方式传输日志：1.直接IP，2.ADSL拨号，3.代理，4，随机路由传输。这里给小菜讲解下，直接IP即拥有公网IP，发表的日志也显示真实的IP，我不推荐这种做法。ADSL上网，ISP会记录下这个IP地址是在哪个特定时间由哪个电话号码上线，你认为这仍然安全吗?代理上网安全么?如果提供代理的主人或是代理服务商与网警妥协，关键是在于网警们有耐心与代理服务商协商。随机路由传输，每次请求传输信息都会透过随机路由进行的每一连串步骤都是经过加密的。此外，在这一连串传输线上的每部电脑都只会知道最邻近的的几台电脑地址，换言之，路由器B只知道路由器A经过它传输网页，而这个传输请求可能又经过路由器C代转。所以，你认为网警能从中找到一丝头绪么?  
  
　　接下来我们来了解网警的在干什么?他们的技术能否对抗社会工程学师。如果读者寻找一些关于计算机取证技术方法及工具研究，我想你会找到最主要的信息，那就是他们重心在于入侵监测系统、数据恢复、加密破解、反向工程技术以及计算机取证软件工具的使用。然而，他们忽略了人为的因素，社会工程学师的奇妙之处在于从人、规章寻找致命的漏洞。且现在面对社会工程学师的攻击防护仍然是网络安全课程的一片空白，当这种攻击趋入严重的状态，这成了网络安全专家首要考虑的问题。然而更令人吃惊的是，网警偶而会发现攻击源来自于他们内部。现在有一些媒体神化了网警，比如一次行动网警现场在网吧抓获攻击者，这并没有什么特别之处，而在于那位攻击者没有隐藏IP，使用的是公用电脑，这对于网警来说更容易确定IP源。行为   
  
　　你相信测谎仪么?不，我拒绝相信!说出这类话的只有两类人，一类是心理学家，另一类便是社会工程学师。  
  
　　这里，我们开始从典型案例说起，那就是广为人知的警'察抓小偷的故事。我们比较关注的是，警,察依靠什么条件来分析谁最像小偷呢?人群中的小偷如何让自已化为一缕空气?这很简单，一旦监控器里的人符合两个明显特征：贼眉贼眼、东张西望，他们以此来判断。小菜们一定碰到过所谓的算命师，他们有种不凡的能力便是，从你的衣着、行为、言语判断你从事何种工作，遇到哪种烦恼。不错，小菜们一定能猜到我想说的：**行为能反映人的状态**。  
  
　　OK，现在我们来谈谈现实与网络里的人的行为。从前面说知，行为能反映人，一旦我们将行为改变呢?北方人操起南方人的口气，不仅衣着举止投足都是一个活生生的南方人，你认为可能吗?当然能，小菜们一定也会列举一些刘德华、张学友等等N多演员，社会工程学里的“伪装”在明星的眼中是“演技”的说法，“演技”人人都会，一旦经过简单的培训，所表现的行为能躲过人的眼睛，小菜们一定认为不可思议，下面给你们一个作业，很简单，和家里人开一个玩笑。模仿你父亲的说话方式给你的妈妈打一个电话，至于目的是什么便自已想了。是的，这稍微会有些难度，那就是口音伪装，社会工程学师才不会在意，随便在网上下载一种变声软件，将所说的话经过变声软件转换输出。嗯?社会工程学师常用的软件或是道具是什么呢?小菜一定这样问，这很简单，只要社会工程学师手上有某物体，他们便会设法利用。  
  
　　最后一个要求便是心理素质，测谎议依据你的说话声音音调以及生理状态作为判断条件，当我们以测谎仪程序的漏洞来测试时，便会出现错误的结果，为什么杀人犯偶尔无法通过测谎仪呢?他们的心情处于极度紧张状态，每一次的回答绝对会打乱他们的心境。社会工程学师在这一方面具有较强的心理素质，若网警找不到一丝证据，主动权仍在于他的手上。  
  
　　网络世界的人又是什么样的呢?小菜肯定为想找一位技术高超的师父来学习，可是只能看见他们在网络里表现非凡的才能，却无法找到他们的联系方式，幸运的一点可能还会被拒之门外，看完本部分开始和高手们开一个小小的玩笑吧。关于“高手”一词，我们得从金庸的武侠名著说起，大师级以上的高手一般会有独门功夫，中级的都设法争夺武林盟主，低纸以下的都是配角了(菜鸟们千万别丢砖头给大菜鸟了)，简单的举例大家都明白高手是什么概念了，中级的一般都会留下名号，不然江湖里的人不知道那就太枉了，大师级的呢一般都是经过N年后故事来传播的，至于菜鸟级的嘛，先买<<黑客X档案>>真经的话3年后就能达到中级，再N年就能达到大师级了，然后....呵，扯远了。  
  
　　武侠里的生活与现实相关，而现实的生活又与网络相关，或说他们有所区别，那只是因为所处的环境不同，但决定性的因素还是人。接下来我们通过几步简单的手法，来一个高手与菜鸟的游戏。准备工作:IM(QQ、MSN、Gtalk)、火狐浏览器(防止一些放马的站点)  
  
　　第一步:寻找目标。这可不能瞎找哦，说话牛头不对马嘴的很快就会被对方踢进黑名单的。小菜可以从这里入手:比如黑X里的作者、论坛、博客，或者一些以原创类性质的站点。  
  
　　第二步:行为分析。这很简单，从目标的作品与言论看出技术水平，以及心理状态，这决定了虽然不能谈论技术但可以成为朋友。  
  
　　第三步:直捣黄龙。直接去加为好友，小菜认为有点难度，不是的哦，非常的简单。如果你以杂志上作者名放到QQ寻找好友的一个以昵称寻找好友的功能，比如我们拿"旭方"来寻找，接下来估计哥们得揍我了(小菜问:旭方是什么?嘿嘿，翻翻后面的几期杂志就明白了)。接下来是论坛，这更简单了，符合金庸的中级侠士定义了，一般他们作品都会留下邮箱、博客，如果点击论坛个人资料，也会看到QQ的，没有?那打开博客来看东西吧，咦?只有几篇看不懂的文章与友情链接嘛，骗人!小菜大骂。如果我们仔细一点，QQ联系仍躲在暗处哦，友情链接打开看看吧，正巧有他的一个哥们留下联系方式了，于是我们一个简单的冒称便弄到目标Q号了。  
  
　　第四步:复制身份:这里是关键了，有的可是设置了身份验证的，首先利用QQ寻找好友的功能把号码填入，查看个人资料。留心他们的个性签名与说明，如果有正在找工作，小菜就把身份改成大企业，如果有的是专于技术，小菜就把身份改成xx工程师....以此类推，成功率满高啦，被拒绝了估计人品有问题了。^-^  
  
　　好啦，行为分析虽小，但五脏俱全。而且偶的Q号可以用上面的方法找到，透露下，菜鸟们也能直接在书上找到黑X编辑的Q号，至于怎么找嘛....(sagi:你敢说出来，这次稿费别想拿了，哈哈。。。)说了这么多，反侦查技术也包含在其中了，攻击者的行为该如何进行伪装。痕迹   
  
　　网络里，能泄露你的隐私主要是:论坛、博客、IM(即QQ、MSN、Gtalk)，**当然，社会工程学师的一切注册信息都是伪造的，因为任何一丝敏感信息都会给网警一个切入点。**至于侵入服务器之类的，他们有时宁愿打一个电话套取密码，也不愿用侵入的动作在主机留下太多的日志，这增加了取证的难度。对这种稍闪即逝的攻击，能留下的痕迹少之又少，在未来的几年，调查取证仍是一个难以解决的问题。  
  
　　反侦查，后门问题。既然侵入主机会留下后门，社会工程学师的攻击不会留有后门吗?答案是确定的。那些后门偶尔会是很简单，他们会在暗处看事态的发展，偶尔会介入制造动作打乱方案。