什么是社会工程学？  
　　定义：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一步地解决各种社会问题。  
　　总体上来说，社会工程学就是使人们顺从你的意愿、满足你的欲望的一门艺术与学问。  
　　它并不单纯是一种控制意志的途径，但它不能帮助你掌握人们在非正常意识以外的行为，且学习与运用这门学问一点也不容易。  
　　它同样也蕴涵了各式各样的灵活的构思与变化着的因素。  
　　无论任何时候，在需要套取到所需要的信息之前，社会工程学的实施者都必须：掌握大量的相关知识基础、花时间去从事资料的收集与进行必要的如交谈性质的沟通行为。  
　　与以往的的入侵行为相类似，社会工程学在实施以前都是要完成很多相关的准备工作的，这些工作甚至要比其本身还要更为繁重。  
　　你也许会认为我们现在的论点只是集中在证明“怎样利用这种技术也能进行入侵行为”的一个突破口上。  
　　好了，其实这样够公平的了。无论怎么说，“知道这些方法是如何运用的”也是唯一能防范和抵御这类型的入侵攻击的手段了。  
　　从这些技术中提取而得出的知识可以帮助你或者你的机构预防这类型的攻击。  
　　在出现社会工程学攻击这类型攻击的情况下，像CERT发放的、略带少量相关信息的警告是毫无意义的。  
　　它们通常都将简单地归结于：“有的人通过‘假装某些东西是真的’的方式去尝试访问你的系统。不要让他们得逞。”  
　　然而，这样的现象却常有发生。  
　　那又如何呢？  
　　社会工程学定位在计算机信息安全工作链路的一个最脆弱的环节上。  
　　我们经常讲：最安全的计算机就是已经拔去了插头（网络接口）的那一台（“物理隔离”）。  
　　真实上，你可以去说服某人（使用者）把这台非正常工作状态下的、容易受到攻击的有漏洞的机器连上网络并启动提供日常的服务。  
　　也可以看出，“人”这个环节在整个安全体系中是非常重要的。  
　　这不像地球上的计算机系统，不依赖他人手动干预、人有自己的主观思维。  
　　由此意味着这一点信息安全的脆弱性是普遍存在的，它不会因为系统平台、软件、网络又或者是设备的年龄等因素不相同而有所差异。  
　　无论是在物理上还是在虚拟的电子信息上，任何一个可以访问系统某个部分（某种服务）的人都有可能构成潜在的安全风险与威胁。  
　　任何细微的信息都可能会被社会工程师用着“补给资料”来运用，使其得到其它的信息。  
　　这意味着没有把“人”（这里指的是使用者/管理人员等的参与者）这个因素放进企业安全管理策略中去的话将会构成一个很大的安全“裂缝”。  
　　一个大问题？  
　　安全专家常常会不经意地把安全的观念讲得非常的含糊，这样会导致信息安全上的不牢固性。  
　　在这样的情况下社会工程学就是导致不安全的根本之一了。  
　　我们不应该模糊人类使用计算机或者影响计算机系统运作这个事实，原因我在之前已经声明过了。  
　　地球上的计算机系统不可能没有“人”这个因素的。  
　　几乎每个人都有途径去尝试进行社会工程学“攻击”的，唯一的不同之处在于使用这些途径时的技巧高低而已。  
　　方法  
　　试图驱使某人遵循你的意愿去完成你想要完成的任务是可以有很多种方法的。  
　　第一种方法也是最简单明了的方法，就是目标个体被问到要完成你的目的时给予其一个直接的“指引”了。  
　　毫无疑问这是最容易成功的，也是最简单与最直观的方法了。  
　　当然，被指引的个体也会清楚地知道你想他们干些什么。  
　　第二种就是为某个个体度身订造一个人为的（通过捏造的手段）特定情形和环境。  
　　这种方法比你仅仅需要考虑到了某个个体的相关信息状况附带更多的因素。  
　　例如如何说服你的对象，你可以设定（刻意安排）某个理由和动机去迫使其为你完成某个非其本身意愿的行为结果。  
　　这包括了远至于为某个特定的个体创造一个有说服力的企图而进行的工作，与大量你想得到的“目标”的相关知识。  
　　这意味着那些特定的情况/环境必须建立在客观事实的基础上。少量的谎言会使效果更好一些。  
　　社会工程学中最精炼的手段之一就是针对现实事物的良好记忆能力。  
　　在这个问题上黑客与系统管理员会更为侧重一点，特别是在某种事物与他们的领域有所关联的情况下。  
　　为了说明上述的方法，我准备列举一个小型的范例。  
　　范例如下，当你把某个个体“置于”群体和社会压力（其类型如舆论压力等）下的处境/形势时  
　　个体很有可能会做出符合群体决定的行为，尽管这个决定很明显是错误的。  
　　一致性  
　　若在某些情况下有人坚信他们群体的决定是对的话，那么这将有可能导致他们做出不同于往常的判断和行为。  
　　比方说如果我曾发表过某个结论，论点的理由非常充分（这里指的是符合群体中多数人的意愿）  
　　那么往后无论我花多大的精力去尝试说服他们，都不可能令他们再改变自己的决定了。  
　　另外，一个群体是由不同位置/层次的成员组成的。  
　　这个位置/层次问题被心理学者称之为“demandcharac-teristics”（“意愿的特征性”），  
　　这个位置/层次问题在参与者的行为上受其浓厚的社会约束性所影响。  
　　不希望得罪其他的成员的、不想被其他人看出自己在会议中想睡觉的、不想破坏与自身关系良好的伙伴的观点等的心态最终都会成为“随波逐流”现象的形成因素。  
　　这种运用到特征的处理方式是引导人们行为的一种有效途径。  
　　情形  
　　无论怎么说，大多数的社会工程学行为都是被一些单独的个体所运用的。  
　　因此诸如社会压力与其它的一些影响因素都必须建立在和目标有一定的可信关系的情况下进行的。  
　　如果处于这样的情形下，当有了真实或者虚构出来的固有特征时目标个体就很可能会遵循你的意愿而工作了。  
　　这些固有特征包括：  
　　·目标个体以外的压力问题。如让个体相信某个行为的后果并不是他一个人的责任。  
　　·借助机会去迎合某人。这些行为更多取决于此个体是否认为某个决定能为某人带来“好处”。这样的行为可以使你与老板的关系更为融洽。  
　　·道德上的责任。个体会遵从你是因为他们觉得自己（在道德上）有义务这么做。  
　　这就是利用了内疚感。人们比较愿意逃避内疚感，因此如果有一个“可能”会让他们觉得有内疚感的话他们都会尽可能地去避免这个“可能”。  
　　个人的说服力  
　　个人的声望和说服能力是一种常被用于促使某人配合/顺从你的有利手段。  
　　使用个人说服力的目的并不是要别人强行接受你所指派的“任务”，而是增强他们对完成你所指派的任务的主动顺从意识。  
　　其实这是有些矛盾的。基本上，目标只是被我们简单地引导到一个已经设置好的、特定的（故意安排的）思维模式上去。  
　　目标会认为他们可以控制住局面，在此同时他们也通过他们的力量帮助了你。  
　　事实上，目标所得到的利益与他间接帮助你得到的利益此两者是没有冲突的。  
　　社会工程师的目的是说服目标，使其有充分的理由去相信只需花费小量的时间与精力就可以“换取”得到利益了。  
　　合作  
　　存在着多个因素可以促使一个社会工程师增加与目标“合作”的机会。  
　　尽量少与目标发生冲突。使用平和的态度去面对对方可以提高达成目的成功几率。  
　　拉拢关系或者发展新的关系，共同的烦恼又或者是一些比较特殊的任务都可以有效地迫使目标与你合作。  
　　在这里‘走向成功’的因素往往集中在你是否有能力去掌握与处理好你的说服力。  
　　这是非常重要的，这一点常被“骗子”（常常使用欺骗手段的人）认为是万试万灵的手段。  
　　心理学研究指出如果人们先前曾经遵照过某个极小的指引而工作（并获得成功）时现在他/她就更可能会去遵照一个更大的（指引）了。  
　　在这里如果曾有过合作的前科的话，那么这次再合作，达成的机会就很大了。  
　　更好的方法是让社会工程学者给予合作对象一些比较敏感的信息。  
　　尤其是一些非常逼真的视听感观，目标能够现场看到或听到你给他们的信息要比他们仅仅可以通过电话听到你的声音更能令他们信服。  
　　这个观点一点也不稀奇，以书写形式或电子方式进行交流的信息是很难让人信服的。  
　　这就如同拒绝某人进行某个IRC风格的通信一样。  
　　关联  
　　不管怎么说，社会工程学运用是否能成功也有取决于目标个体与你的目的有多大关联的因素的。  
　　我们可以说系统管理员、计算机安全执行官、技术研究人员、那些依靠计算机和网络进行工作又或者通过其进行通信的人与大多数黑客使用社会工程学进行攻击的目标都是有莫大的关联的。  
　　有高度关联性的个体大多会被强而有利的论据所说服。  
　　事实上你可以给予他们更多强而有利的论据来支持你的观点。  
　　当然，那些观点也有薄弱的一面。你是否将论点薄弱的一面展现给有高度关联的人知道将极大可能地决定你是否能说服此人。  
　　当某人有可能直接被社会工程学攻击所影响，若此时出现薄弱的论据将有可能会导致其思想上产生“相反”的意识。  
　　所以面对与你的目的有关联的人时你必须给予强而有力的论据，而避免出现理由薄弱的论据。  
　　相对于对你的指引或你想得到的结果并不敢兴趣的人，你可以把他们列入“低关联的人”这个类别中去。  
　　相关的例子如：一个网络系统机构中的保安人员、清洁工人、又或者是前台接待小姐等。  
　　因为低关联类别的个体并不会直接对你的目的/结果造成影响，而且他们往往不会去分析你用来说服他们的论点的双面性问题。  
　　他们的决策往往会遵循你的意愿又或者是完全不受其它的“意识”所影响。  
　　这些的“意识”如：社会工程学所提供的理由、表面形势上的迫急性又或者是在某人强烈的说服下。  
　　凭经验而论，在这样的情况下我们只能尽可能地给予其更多的论据与理由了，估计这样的效果会更好一些。  
　　基本上，对于那些与你的意识不一致的人，试图用大量的论据和指引去说服他们更胜于他们与你的目的的关联程度。  
　　有一点是需要注意的：在进行某些工作的时候，能力低的个体更多会去仿效能力高的个体的行为模式。  
　　在计算机系统管理方面，“能力低的个体”大多是指上文所提到的“低关联的人”。  
　　站在上述的观点上考虑，不要试图对系统管理员这类别的个体进行社会工程学攻击，除非其能力不及你，不过这样的可能性非常的低。  
　　防御他人的攻击  
　　综合上述的资料能否让读者更好地保障他们整个计算机系统的安全呢？  
　　其实踏出“美好的”第一步就是要视乎员工们能否在自己的工作岗位上保障自己的计算机系统的信息安全。  
　　这不但需要你无条件地增强他们的安全防范意识，而且你自身也必须具备更高的警惕性。  
　　打个比方，如果你让某人专门负责保护你的计算机系统安全的话，那么就有便利于那个人在没有正常许可的情况下访问你系统的可能了。  
　　无论如何，对付与防御这类型攻击的最有效手段，也作为最常见的手段，就是“教育/培训”了。  
　　第一步是教育你的雇员与那些有可能被利用作为社会工程学实施目标的人关于计算机/信息安全的重要性。  
　　直接给予容易攻击的人们一些预先的警告已经足以让他们去辨认社会工程攻击了。  
　　不过要记着，在教育他们计算机信息安全的时候可以使用一些故事及其“双面性”来作为例子。  
　　这并不是我自己的个人喜好哦。当个体明白了这个焦点的“双面性”以后他们基本上就不会动摇他们所处的立场了。  
　　而且如果他们是专注于计算机安全技术的话，那么他们更有可能会站在维护你的数据安全的立场上。  
　　也有不会遵从人们的说服力倾向而作出行动的思维因素的。  
　　在这里你必须有清晰的思维、高度的创造力、可以应付和处理压力的能力与适当的自信。  
　　压力的处理能力与自信可以通过后天培养。  
　　至于自身的主张和见解常常被用于对员工的管理方面，训练它可以减少某些个体被施行社会工程学攻击的机会，也有助于其他方面的工作。  
　　了解各种使人们的信息安全意识降低与威胁你的安全策略的因素。  
　　其实这方面只需要投入小量的精力就可以在降低安全风险方面产生很大的成效了。  
　　结论  
　　与普遍的思想观念相反，运用社会工程学捕捉人们的心理状态的技巧要比入侵一个邮件服务器容易得多。  
　　但如果你想让你的员工去预防与检测社会工程学攻击的话，其效果绝对不会比你让他们去维护UNIX系统安全的效果明显。  
　　站在系统管理员的立场上，不要让“人之间的关系”问题介入你的信息安全链路之中，以至于让你的努力前功尽弃。  
　　站在黑客的立场上呢，当系统管理员的“工作链”上存放有你所需要的数据时，千万不要让他“摆脱”自身的脆弱环节。  
　　社会工程学（Social Engineering）  
　　一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段。  
　　取得自身利益的手法，近年来已成迅速上升甚至滥用的趋势。那么，什么算是社会工程学呢？  
　　它并不能等同于一般的欺骗手法，社会工程学尤其复杂，即使自认为最警惕最小心的人，一样会被高明的社会工程学手段损害利益。  
　　社会工程学陷阱就是通常以交谈、欺骗、假冒或口语等方式，从合法用户中套取用户系统的秘密。  
　　社会工程学是一种与普通的欺骗和诈骗不同层次的手法。  
　　因为社会工程学需要搜集大量的信息针对对方的实际情况，进行心理战术的一种手法。  
　　系统以及程序所带来的安全往往是可以避免的。而在人性以及心理的方面来说。  
　　社会工程学往往是一种利用人性脆弱点、贪婪等等的心理表现进行攻击，是防不胜防的。  
　　借此我们从现有的社会工程学攻击的手法来进行分析，借用分析来提高我们对于社会工程学的一些防范方法。  
　　熟练的社会工程师都是擅长进行信息收集的身体力行者。  
　　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，都可能会被社会工程师所利用。  
　　在猫扑网上发现流传着一句话，那就是我们所说的→人肉搜索达人，社会工程学身体力行者。  
　　最近NOHACK出了新书《社会工程学》，作者是范建中，大家可以做为参考