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。   
　　通常在对一个纯静态页面或者服务器和网站程序都不存在安全漏洞的网站做安全检测的时候我们采取的办法就是入侵C段服务器然后继续渗透，但是这样的办法面对一些独立机房的服务器就束手无策了，所以我们引入社会工程学做安全检测！  
　　通过对网站工作人员的社会工程学欺骗手段获取网站相关管理信息——服务器密码、SQL数据库密码、FTP密码、网站管理后台地址、网站管理密码等。假如没办法直接获取Web服务器及Sql服务器的权限资料，我们就要将目标锁定在公司内部员工及管理层的电脑 权限上了。通过社会工程学手段获取公司员工资料及联系方式（姓名、电话、生日、qq、邮箱、电话等）。当我们获取这些重要信息的时候我们离服务器权限已经很近了！   
　　为了方便大家更好的理解我所说的安全检测过程，我画了张简单的结构示意图：  
　　如图我们来看下哪些人为因素可能导致安全问题：  
　　1. 服务器管理人员的专业素质  
　　2. OA系统中的成员素质  
　　3. 企业对涉密资料保密措施  
　　4. 人员数据流动传输介质的管理防护  
　　5. 人员间的联系及操作审核  
　　接下来我们来详细说明下如何通过这些可能导致安全问题的人获得更多的资料和权限。  
　　这里我由易到难逐一进行说明。再进行下面具体的社会工程学渗透之前我们要先收集一定的资料例如：  
　　网站运营公司名称、地址、所有联系方式、服务器IP段、服务器所在机房、机房工作人员资料、公司工作人员资料（包括公司高层管理人员及服务器管理人员）、域名、域名购买地点、域名所有人信息、域名注册邮件地址  
　　公司和网站域名得相关资料都很好获得，这里就不做详细说明了。我们这里重点讲如何获得人员联系方式：   
  
　　首先是网站所在服务器IDC机房人员资料：  
  
　　通过前面搜集服务器所在IP段我们可以通过直接访问IP得知服务器提供商。例如你访问北京万网服务器机房的服务器IP的时候都会看到万网服务器的广告页面。那么我们就可以确定所在机房信息，接下来就是到服务器提供商的网站上查找工作人员资料。最容易得到的人员资料当然是网站客服人员。人员又分为售前和售后，通常售前都是一些专科毕业的MM，她们的计算机专业知识及安全意识都是非常薄弱的，但是要最快的得到服务器权限当然还是要针对售后客服，售后客服又分GG和MM ,GG当然是负责服务器维护的工作人员，对服务器拥有直接的操作权限。MM是负责解答客户问题和向GG提交问题的。所以要得到服务器权限这里可能就要去社会工程学得到GG和MM的电脑权限。相对拥有专业知识和安全意识的GG 那些安全意识薄弱的MM相对好对付很多。想象下，你发任何文件给服务器管理人员他都不会轻易运行。哪怕是一个Word 0day。可能也会因为管理员本机每必更新的杀毒软件而葬送，而且马上就会引起对方的警觉，那么计划就立刻落空了。相信1一个小时内你发送病毒文件的事情真个机房的工作人员都知道了，可以打保票至少一个星期内你想对任何一个人进行社会工程学欺骗都不可能了。  
  
　　所以我们的第一目标应该是负责售后联系的MM，例如我们和客服联系的时候告知对方我们的网站无法访问了，那么对方一定会开启你的网站进行访问验证是否真的无法访问了。如果你能构造一个非常逼真的网站出错的网马页面（前提你的网马最好是0day或者免杀的比较流行的第三方软件漏洞），当客服MM发现你提交的网站地址确实出错，而且她自己无法为你及时处理的时候，她就会把你给她看的地址发给负责服务器维护的GG，运气好的话这个时候你就可能得到客服MM的电脑权限或者服务器管理员GG的电脑权限（如果管理员直接在服务器上访问你的页面，而且你的网马是系统级别的漏洞那么很可能可以直接得到服务器权限）。  
  
　　如果你运气没有那么好或者没有一个好的免杀的网马而不敢进行这样的尝试，那么你可以选择对客服人员进行另一种社会工程学入侵——诱骗对方接受并运行你的文件（例如：Word、Excel、PDF、RAR甚至是EXE文件等），那么到底如何诱骗对方接受且运行你的文件呢？下面我们就来简单的介绍一下：  
  
　　想要客服人员运行你的文件有简单的办法也有困难的，简单的办法当然是发送Word文档谎称这个是一个域名变迁表格之类的文档（当然要先和对方取得联系，先要求对方发送一份表格给你，就说是在别的地方买的域名想要转到他们这里来续费，这里我试验过，对方一定会发一份表格给你要求你填写，就是域名转入申请表。接收这个表格以后佯装填写一段时间，切忌不要太长！假如你早上填写的表格，下午才发换给她，到时候MM未必记得那个表格是她发给你的，那样就不会毫无戒心的运行了。）这样就顺利得到MM电脑的权限，你从她电脑得到很多有用的信息——例如：MM的QQ账号密码、IDC网站上的后台账号密码、公司内部FTP密码（如果有上传权限当然最好,这样你就可以在他们公司的内部资源里捆绑一些木马，这个方法同样适用于公司的内部群，这个也有很大机会得到公司内部其他人机器权的）、公司其他成员资料（Email、电话或者qq）等……接着你可以利用这里搜集来的资料和权限进一步扩大对IDC机房内网的控制。  
  
　　例如你可以进行内网映射。把自己的机器映射到对方个公司内网，然后扫描内网肉鸡。运气好的话直接得到服务器管理人员电脑权限、或者公司管理层电脑权限。前面我们已经说过。如果你可以得到上面2种人的电脑权限，那么距离服务器的密码和权限就已经很近了。  
  
　　你也可以偷用MM的qq趁下班时间和尚在服务器机房值班的GG联系，欺骗起运行你的病毒文件、或者开启带毒网站（GG的值班表从公司的内网中可以找的到），接着如何利用MM的身份让GG点你的带毒文件？这里看就看你的社会工程学入侵经验和技术了。这里我提供集中思路：  
  
　　1：佯装发送照片（谎称最近出去游玩拍的，因为文件太多四所以进行打包压缩，而压缩文档则为带毒文档）  
　　2：发送Offiece文档（佯装小说、或公司资料、客户要求等……）  
　　3：发送网址（佯装帮MM参加的某活动投票,这里要自己构造一个欺骗页面，网址中最好包含一些投票、选美之类的中文拼音作为文件夹名称）  
　　4：……  
  
　　此外，前面说到如果得到公司网站的后台管理密码（客服一般都会有一定的后台权限，哪怕很小的权限，只要是后台，也可能暴露很多重要的信息——例如：暴露后台新闻公告发表页面的Html编辑器是存在漏洞的eWebEditor或者FckEditor等…曾经遇到过一个网站程序普通管理员居然具有编辑数据库连接参数和网站资料的权限，而这些参数和资料恰巧保存在一个实体的网站程序里（也就是说可以写文件），这样我们就可以手工构造一个一句话木马从而得到公司Web服务器权限）。假如能从这里顺利得到Web服务器权限的话，可以轻松的从个服务器里得到客户资料，也就是我们的目标用户的网站Ftp密码、域名管理密码、服务器管理密码等有用信息。这样一来即使我们无法提升服务器权限然后进行机房内网嗅探，也可以顺利拿下目标站点。  
  
　　同理，如果从MM和GG的社工失败，还可以尝试其他途径，也就是上面说到的对服务器有最终权限的人——公司管理层。  
　　设想，如果你的老板发公司邮件给你。或者在MSN或者qq上告诉你他的后台密码忘记了、或者目标站点的领导委托他让你在服务上添加一个FTP账号或者系统账号，你敢说No吗？o(∩\_∩)o…明白了这个简单的道理，我们的进一步渗透就有了目标。通过从MM电脑和公司内网或者其他途径搜集来的公司人员资料里，尽可能多的找出领导层资料。利用这些资料社会工程学入侵、或破解他们的qq、Msn、或者邮箱。  
　　这里顺便再提供下获取公司人员邮箱的办法：一个是内网得到的信息，另外一个通过对公司网站路径的扫描。有的时候可以发现一些不对外开放的公司内部论坛。可以从公司论坛上得到管理层的ID和邮箱，运气好的话还能直接通过这个内部论坛的漏洞获取公司网站权限或者数据库（数据库中保存公司所有人员的常用网名ID、密码、邮箱、生日等重要信息）  
　　得到这些资料就要对邮箱、qq、MSN等进行集中社工或猜解，然后就是利用得到的账号想服务器维护人员发送命令，接着当然就是很邪恶的拿到权限了…  
　　上面介绍的方法同样适用于对目标站点公司的社会工程学入侵及渗透，在社工目标公司的时候由于客服不会像IDC机房里的客服人员一样很轻易的打开你传给他们的文件，所以这里就出现了一个问题——如何让目标站点的公司人员运行你的病毒文件。这里以软件或游戏公司为例：  
　　假如我们要得到某个收费软件公司的内网权限。那么你可以从他们的网站上得到他们公司售后客服人员的联系方式，例如一个邮箱、qq等。然后告诉对方“你购买了他们的软件或者安装了他们的游戏，可是不知道为什么老出错，麻烦你帮我看下到底怎么回事（这里你就可以发送一些压缩文件、Word文档或者发送一个捆绑了木马的对方公司软件或游戏主程序），有些时候客服人员觉得这样的邮件每天都有好多，所以不加理会。  
　　要让这样的客服人员打开你的文档，就要进行骚扰、甚至使用激将法。也就是说很可能这个时候你需要使用大量的虚假邮箱发送各种邮件诱使对方打开，只要对方上当打开其中一个，很可能你就顺利得到对方电脑的权限了。至于激将法——也就是要采取一些辱骂性的语言，表达自己问题迟迟得不到解决而愤怒的心情。相信当客服人员遇到这种情况的时候最终一定会被你征服，哪怕只是一丝的怜悯之心，也可能带来这场欺骗战的胜利！顺利得到客服电脑权限后依然是按照我们上面说的办法继续对公司内网进行进一步的渗透，渗透的过程是非常漫长的，需要很大的耐心和细心。有的时候甚至会把公司内网每个人的电脑上的文件都翻一遍，甚至要下载庞大的数据到本地进行分析…  
  
　　方法说起来虽然就简单的这么些内容，实际操作起来确实非常漫长和费时费力的。最后还是看大家多实践和灵活应用，当你成功利用上面的办法得到一个一直无法拿到的网站的时候，你就会知道社会工程学的强大！