原文出自:<http://heik.cn/n126c11.aspx>  
　　我们很多时候在入侵，在得到webshell，甚至是服务器系统权限的时候并不知道这些权限意味着什么。我们很多时候在面对一个目标的时候，只单纯的运用一些所知甚少的技术漏洞去尝试入侵，在周而复始的重复劳动中慢慢丧失渗透的激情和信心。  
  
　　下面我举个简单的例子：  
  
　　很多朋友喜欢盗QQ号码。我这里就以盗QQ为例来说一些社会工程学的应用。  
  
　　声明一点：我本人并未盗过任何人的QQ号码，尽管有时会做些测试，但最终会归还失主。我这里也竭力反对朋友们盗别人的号。  
  
　　question：盗qq号？  
  
　　如何盗？有几种途径？各种方法又是如何实施的？  
  
　　从形式上看盗号无非几种方式：  
  
1 入侵式－系统被入侵或者中马，采用键盘记录类获取别人的QQ密码  
2 爆破式－采用一些爆破工具大面积爆破简单密码QQ号  
3 钓鱼式－制作一些挂机，赠Q币的假网站，欺骗QQ用户登陆，获取密码；大量发送带马邮件或者恶 意网页，引诱上钩  
4 社会工程学延伸破解－大多是邮箱破解  
  
　　针对以上4种方案分别分析：  
  
1 入侵式  
适用指定目标，掌握一定信息。对个人机子而言结合社会工程学效果更佳。  
缺点是一旦对方安全意识较好，很难突破。  
  
2 爆破式  
范围广，爆破机器性能要求高，只能爆破出一些弱口令号码，本人不太喜欢。  
缺点是费时费力，盲目性突出。  
  
3 钓鱼式  
此招适合一些具备相当技术功底的人群，危害也极大，成功率高，普通网民容易中招。  
缺点，技术含量要求较高，守株待兔式。成功率的高低也取决于鱼饵设置的“逼真”程度。对设置陷阱者本人综合素质要求高  
  
4 社会工程学延伸破解  
适用范围广，适合稍具技术知识的菜鸟，成功率也较高。缺点是周期长，在于积累。  
  
　　我这里着重将一下第四种方式：  
  
1 入侵一些有明显安全漏洞的论坛或网站  
2 下载论坛或网站的数据库  
3 导出数据库中注册用户：用户名，密码，QQ，邮箱，密码问题，问题答案，生日等敏感信息  
4 挑选破解一些看种的QQ号码  
  
　　其实写到这里，大伙也该明白思路了。网上有漏洞的bbs，网站一堆一堆的。朋友们手头的webshell也又有其他用途了。数据库的重要性，社会工程学的延展性，灵魂运用，扩散思维，恐怕倒时6位7位的QQ号已经不是什么难事了。  
  
　　还不明白？  
  
　　密码可能通用嘛！不通用也不要紧，还有密码问题嘛！还不行？咱还有邮箱呢，利用忘记密码功能，把修改密码的邮件发到已经破解的邮箱里，嘿嘿！还不行？生日也很有用哦......不说了，说这么明星没意思了。  
  
　　以上我以盗QQ号为例，说了一些技术与思维相结合的盗号方式。目的不是在教大家如何去盗QQ这么狭隘，大家不妨想得远些，能做的事情多着呢。