常见密码破解技术

1、暴力穷举

密码破解技术中最基本的就是暴力破解，也叫密码穷举。如果黑客事先知道了账户号码，如邮件帐号、QQ 用户帐号、网上银行账号等，而用户的密码又设置的十分简单，比如用简单的数字组合，黑客使用暴力破解工具很快就可以破解出密码来。因此用户要尽量将密码设置的复杂一些。

2、击键记录

如果用户密码较为复杂，那么就难以使用暴力穷举的方式破解，这时黑客往往通过给用户安装木马病毒，设计“击键记录”程序，记录和监听用户的击键操作，然后通过各种方式将记录下来的用户击键内容传送给黑客，这样，黑客通过分析用户击键信息即可破解出用户的密码。

3、屏幕记录

为了防止击键记录工具，产生了使用鼠标和图片录入密码的方式，这时黑客可以通过木马程序将用户屏幕截屏下来然后记录鼠标点击的位置，通过记录鼠标位置对比截屏的图片，从而破解这类方法的用户密码。

4、网络钓鱼

“网络钓鱼”攻击利用欺骗性的电子邮件和伪造的网站登陆站点来进行诈骗活动，受骗者往往会泄露自己的敏感信息（如用户名、口令、帐号、PIN 码或信用卡详细信息）,网络钓鱼主要通过发送电子邮件引诱用户登录假冒的网上银行、网上证券网站，骗取用户帐号密码实施盗窃。

5、嗅探器（Sniffer）

在局域网上，黑客要想迅速获得大量的账号（包括用户名和密码），最为有效的手段是使用 Sniffer 程序。Sniffer，中文翻译为嗅探器，是一种威胁性极大的被动攻击工具。使用这种工具，可以监视网络的状态、数据流动情况以及网络上传输的信息。当信息以明文的形式在网络上传输时，便可以使用网络监听的方式窃取网上的传送的数据包。将网络接口设置在监听模式，便可以将网上传输的源源不断的信息截获。任何直接通过 HTTP、FTP、POP、SMTP、TELNET 协议传输的数据包都会被 Sniffer 程序监听。

6、系统漏洞

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。许多系统都有这样那样的安全漏洞，其中某些是操作系统或应用软件本身具有的，这些漏洞在补丁未被开发出来之前一般很难防御黑客的破坏，还有一些漏洞是由于系统管理员配置错误引起的。这都会给黑客带来可乘之机，应及时加以修正。利用系统漏洞的攻击手段所以能够存在，根本原因是系统中有安全漏洞的存在以及人类在使用中所犯的错误所致。因为很难保证系统的实现和使用中发生错误，所以从理论上说无法从根本上解决系统攻击问题。但是因为系统攻击依赖于系统中存在的各种漏洞，尽量消除系统中的漏洞并同时严格用户的行为，努力将人为的错误风险减少，可以将系统遭受攻击破坏的可能性减小到最低限度。

7、远程攻击

远程攻击是指通过网络对连接在网络上的任意一台机器的攻击活动。一般可根据攻击者的目的粗略分为远程入侵与破坏性攻击两部分。典型的远程入侵，是指入侵者通过网络技术，非法获得对目标系统资源的最高控制权。使用远程控制木马监视用户本地电脑的所有操作，用户的任何键盘和鼠标操作都会被远程的黑客所截取。破坏性攻击则是以盗窃系统保密信息、破坏目标系统的数据为目的。

8、不良习惯

有一些公司的员工虽然设置了很长的密码，但是却将密码写在纸上，还有人使用自己的名字或者自己生日做密码，还有些人使用常用的单词做密码，这些不良的习惯将导致密码极易被破解。

9、绕过破解

绕过式密码破解原理非常简单，其实就是绕过密码的认证机制，绕过的方法有很多种，有些取决于系统本身，有些和用户的习惯有关，例如用户如果使用了多个系统，黑客可以通过先破解较为简单的系统的用户密码，然后用已经破解的密码推算出其他系统的用户密码，而很多用户对于所有系统都使用相同的密码。

10、密码心理学

不需要工具而破解密码的骗局称为社交工程攻击。很多著名的黑客破解密码并非用的什么尖端的技术，而只是用到了密码心理学，从用户的心理入手，从细微入手分析用户的信息，分析用户的心理，从而更快的破解出密码。其实，获得信息还有很多途径的，密码心理学如果掌握的好，可以非常快速破解获得用户信息。