攻击手法

在我们做渗透的过程中，往往通过员工能搞定很多的企业，拿到核心的数据库，最常见的如以下几种情况。

1.密码一条龙

由于很多的互联网数据库被黑客入侵，在互联网或地下圈子流传，通过信息查询到某个公司员工邮箱，电话，姓名等可以从社工库查询到已使用的密码，而所有网站及公司系统使用的账户都同属于一个密码，给攻击者带来了很多的便利条件。

2.安全意识薄弱

通过信息搜集到邮箱等信息，发送一些诱惑力文件，员工会不会判断是否木马,从而进行打开、让攻击者直接获取个人电脑权限。

3.弱口令 默认口令

弱口令，密码跟账户名相同，或者为密码为账户名之后加 123、如 wangjun,密码 wangjun123.或者常见的弱口令,admin 1q2w3e

通过第三方漏洞平台，或者已登录到某个邮箱查看默认密码,很多公司给新人入职的时候都会设置一个默认的密码，如 aabbwangjun，这样设置存在规律。

4.公开分享

如 github 百度文库这些都属于公开的内容，而传源码的时候，没有进行脱敏处理，自己的常用密码，或者公司的敏感信息存在。

5.网盘 云笔记

当网盘，或者云笔记存在漏洞，或者攻击者知道你密码的情况下，进入你的网盘，获取到已存储的敏感信息。

6.私建 wifi

有的公司 wifi 有 mac 地址绑定，这样的情况下员工的手机没办法上网，这时候很多人自己建立 wifi，切密码为弱密码，或者根本没有设置密码，攻击者在你公司一定的范围

内，可以破解无线密码，通过你的电脑，当作一个跳板,来连接到公司的内网。

7.资料脱敏

某天，接到邀请，去参加某个大会，让你来做一个 PPT，ppt 中出现了你公司的网络拓扑，或者是某个系统版本型号，知道拓扑我就知道你内网环境，知道系统版本型，我可以对应版本型号去找下漏洞，往往内网系统很多的漏洞都没有修复。

8.敏感信息保存

如密码就保存在某个盘符，文件名就是 xxxx 密码.txt。或者某些公司敏感的文档应该加密保存。

9.私建 web

程序员写代码为了调试兼容性运行一套集成化的环境，如 phpstudy，但这些环境的密码都是默认密码并且服务都是 system 权限，攻击者可以直接连接你数据库获取你的电脑权限，还有很多的人运行一套存在漏洞的系统，这时候也给攻击者带来便利条件，如 jenkins wampserver 等。

10.禁用缓存密码

如现在很多的软件，都会提示让你保存密码,为了下次不输入密码。看起来很方便，提高了用户体验，但往往也存在安全性，因为你保存密码，那么肯定会存储某个地方，如注册表，安装目录配置文件等，很多的加密都是可逆的，如 chrome ,winscp 等。

11.sns 暴露真实信息

1.认证　　可得知认证公司极职位

2.教育　　可得知曾经的教育经历

3.职业信息　可得知曾经的就职信息

4.个人简介　可得知到你的电话，邮箱，博客等一系列信息

防御方案

公司层面

按时修改账户密码，切密码为大小写数字字母混合，长度为 8 位，公开演讲的 PPT 进行内审。监控系统，监控外部公开分享是否存在我司敏感信息，wifi 安全，推荐 360 天巡(发现伪热点，进行阻断)。Wifi 这块暂时了解到就这么一款比较成熟的产品。

个人层面

密码分为 高 中 低设置不同的密码，

mail 支付宝 QQ 等我列为一类为高危，因为一旦获取到账户之后，可以获取大量的真实的信息。

网盘 云笔记 列为一类为中危，不在这些地方储敏感信息，因为我这时候有可能有自己的一些总结笔记，

低危,很不常用网站，注册的时候就使用最简单的密码如 123456 等，登录进去也无所谓，没必要设置高强度的密码。

家庭地址：

每次买东西都填写一次家庭地址，不会把家庭地址保存京东 淘宝等。

缓存密码:

不在任何浏览器缓存任何网站的密码，定时清理下访问记录。

本地搭建 web 服务

只允许本机访问，这是我一贯的作风，要是同事可以访问可以指定 IP。或者你的密码必须为高强度。