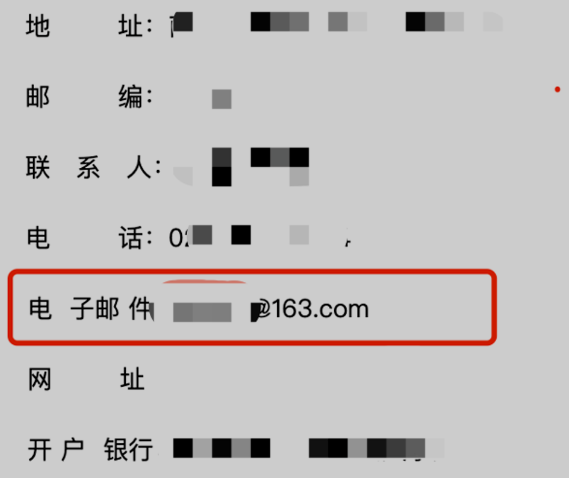
* **案例1--招标平台二级跳**

某央企项目，在其招标采购网进行联系人搜索，找到一个供应商邮箱。

  
通过之前互联网公开的泄露数据查询该联系人电话，查出密码成功撞进邮箱。在该邮箱中发现了目标单位采购部人员联系方式。

文本

描述已自动生成

**继续使用之前互联网公开的泄露数据查，运气好又成功了，这样实现了从招标平台到企业邮箱的二级跳。**

图形用户界面, 应用程序, Teams

描述已自动生成

翻看附件，通过一系列搜索找到一处页面。

卡通人物

中度可信度描述已自动生成

下载然后反编译找到地址最后获取shell。

* **案例2--爱企查隐藏的惊喜**

某HW项目，找到oa页面。一开始拿exp打没有效果（后来发现是exp弄错了，尴尬），短暂陷入僵局。



以前的我遇到这种exp打不进去就会直接放弃，现在不同了，我会简单尝试猜一下弱口令，碰下运气。用户去哪儿找呢？我将目光放到了爱企查。在页面中查到公司主要人物，我打算每个人都试一下，密码就是123456，111111，全拼+123456，全拼@123456之类的。

图形用户界面, 应用程序

描述已自动生成

结果运气还真来了，试到第二个就进去了。

图形用户界面, 文本, 应用程序

描述已自动生成

进了oa，权限还挺大，所以后续波澜不惊正常操作，泛薇exp也成功利用，基本上打穿了。但是还差一台比较重要的服务器。

当时情况是这样，通过抓取获得两个通用密码：

administrator/456rty$%^20170106

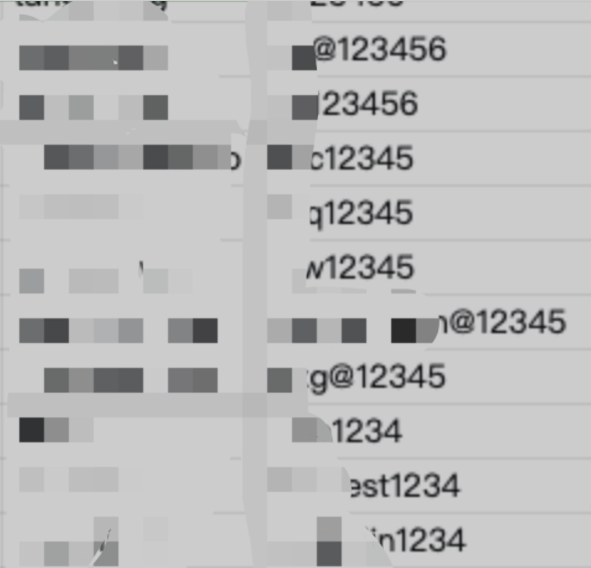
administrator/123qwe!@#\_fwq

这两个密码基本上通杀内网里面的服务器，路径分刷的差不多了。但是还有一台重要服务器不能用，这时候就只有硬猜了。

这两个密码规律都是跟键盘有关，后续跟的内容跟时间和公司有一定联系。所以排列组合一下最终猜出了正确答案：administrator/456rty$%^

* **案例3--邮箱爆破到内网**

国内某知名上市软件企业攻防项目。这个项目严格来说是看大佬操作，正是这个项目学到了邮箱爆破的思路。信息搜集一番后，虽然目标资产很多，但是没找到啥突破口，毕竟目标也是it公司，对安全这块也很重视。还好运气不错，在领导给的联系人中通过之前互联网公开的泄露数据找到一个密码，登上了邮箱。不过该人员属于业务部门，邮件中没有什么对我们有价值的内容。怎么办呢？当然第一步先把通讯录导出来，导出来后，大佬一波突突，顺利找到多个账号，爆破原理就是通过对姓名声母韵母的拆分，外加123，12345等常见后缀形成的弱口令，结果如下

登录这些新账号，慢慢搜索，最终另外一位大佬找到一处隐秘地址存在shiro漏洞，进了内网，后续一路靠着搜集来的密码和key控制了云主机管理平台。

* **案例4--不靠系统漏洞，从外网获取域控**

国内某上市网络服务提供商攻防项目，提供了ip地址，不准钓鱼。先是照着上面信息搜集的方式，在github上先有了收获。

日程表

描述已自动生成

登录了后发现这个邮箱是个海外的客服邮箱，当客户请求密码重置的时候这个邮箱可以发送重置链接，所以理论上可以获得任意客户的账号。

图形用户界面, 应用程序

描述已自动生成只是这个邮箱对应的域名和其网站提供的服务属于对外业务，跟我们初始目标有一定差距，确定方向偏了后就没再深入挖掘。

接下来是扫描客户给的自用ip段。

找到一个站点，在邮件通知处发现泄漏的账户和密码。用f12查看隐藏的密码。图形用户界面

描述已自动生成

登陆邮箱成功，邮箱中发现vpn地址（办公区域）。

文本

中度可信度描述已自动生成

邮箱垃圾箱中发现邮箱每天接收的routerOS的配置文件备份，其中有其他vpn的连接密码(生产区域)。

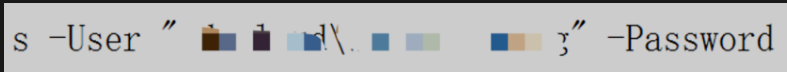
QR 代码

中度可信度描述已自动生成

登陆第一个办公区域的vpn后才能登陆第二个生产区域vpn。此后攻击链分成两路，分别对生产区域和办公区域进行渗透。

后面操作就是上述提到的，对每个内网主机的文件都不放过。

在生产区域内，在某一台运维机上，发现运维脚本，上面有域控账号的密码，但是上面的密码过期了。



这是今年1月份的密码，尝试之后发现失败。但是结合原本密码猜测，如果要改就是把xxx@2013;1改成xxx@2013;2，以此类推，按半年改一次的话，现在7月，不是2就是3，尝试连接成功,密码是xxx@2013;3。至此生产环境域控权限拿下。

图形用户界面

描述已自动生成

转战办公环境，虽然通过单点登陆进入了很多内部系统，但是系统中没有漏洞，办公内网个人机防护也到位，始终无法获取shell。

这里因为缺乏经验卡了很久，幸好在神秘高人的帮助下，然后内网所有信息都全部集齐生成了密码本，成功爆破zabbix服务进入后台。

有了zabbix的后台，直接提升一个普通账户为域管，后续波澜不惊的拿下生产环境。

图形用户界面, 应用程序

描述已自动生成

信息搜集始终是最重要的。这篇文章谈了谈信息搜集和密码利用的思路，但是这类思路不是万能的，很多时候需要运气，成功率也不高，只是给大家在没有突破的时候提供一点启发，更多还是要靠自己打牢自己的基础去找漏洞。