1.背景

最近在进行一些红队评估项目，并取得了一些还不错的成果，但是在这过程中，发现团队刚毕业新来的小伙伴在这过程中都没有找到我发现的这些资产，其实漏洞谁都会利用，但是难就难在打点中，所以趁这段时间不忙，写一写我平常在针对某个行业、某具体单位的打点方法，希望能对一些实战经验不多的师傅们提供一些思路，如果师傅们还有更好的思路，欢迎探讨交流。

2.目标

在市HW中，你可能会拿到几十个甚至上百个目标，大点的会有政府单位和上市企业，小点公司只有一个阿里云资产，有的甚至是某个小学、某个社区服务站(亲身经历)，小到根本没有外网资产。我*****，你让我怎么打?

省HW、国HW中，队伍分配的目标就是省行业主管单位、国企、上市企业等等，都是比较大的单位（但是也有部分单位没有互联网资产，只能靠一个招聘邮箱钓鱼，也有大佬钓成功了的，tql）

还有平时接一些政企单位自己整的攻防演练，这个只能叫红队评估，目标比较明确，不会太分散。其实每次红队项目都能遇见不同的目标，而且很多时候是有大量的目标，而且时间比较短，这就非常考验红队队员的打点能力。

3.打点的基本方法

方法说起来很简单，无非就是信息搜集—漏洞利用—getshell。但是最难，最耗时间的就是信息搜集，纯牛马体力活，这过程中也可以利用一些工具，但是工具只是一个辅助，还是要靠大量实践去积累经验。然后你才能比人家发现更多的资产。话不多说，思路大家都懂。

4.打点的艺术

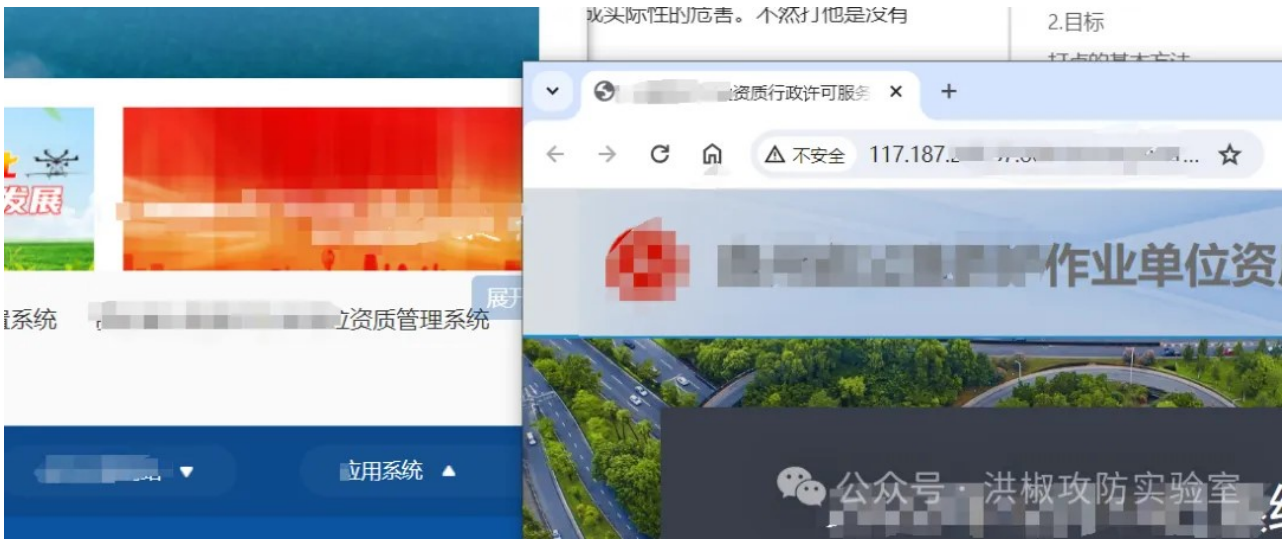
首先，我们要看我们的目标是什么，部委？省市某行业主管单位？还是某个大型企业？要对目标有一个基本的认识，有多少下属单位，涉不涉及大量个人信息等等。

最简单的方法就是去官网，看该单位的组织架构；去企查查看单位的持股结构、对外控股企业等等。还得思考控股企业能不能对主要目标造成实际性的危害。不然打它是没有意义的。

4.1.官网

拿到目标后第一时间去看它的官网，从官网就能了解这个单位有哪些下属单位，因为单位与单位之间的网络一般都是互通的。还有的时候可以从官网获取到部分资产信息。比如：

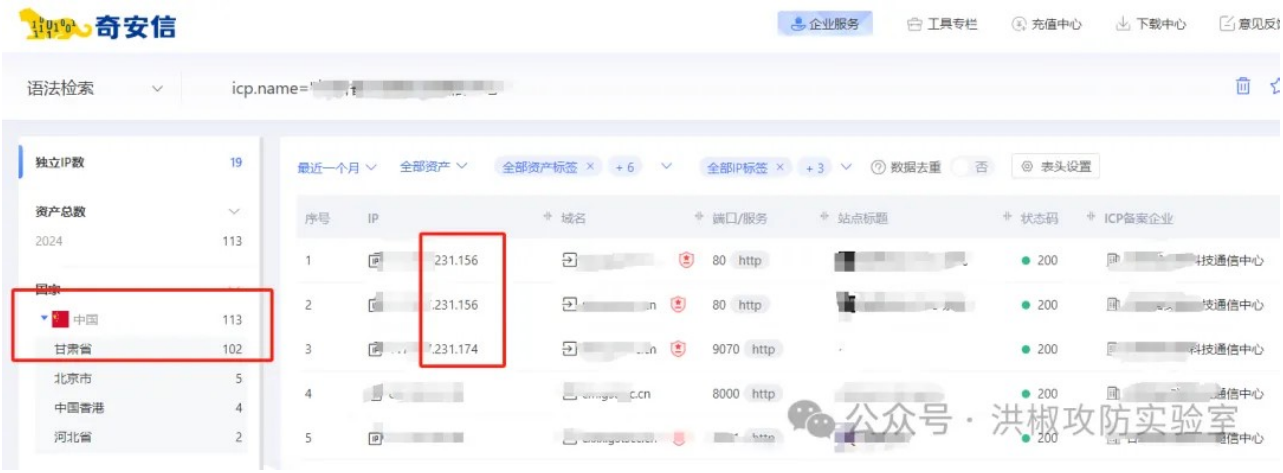
有时候能发现一些用Title、备案号等等查不到的系统。



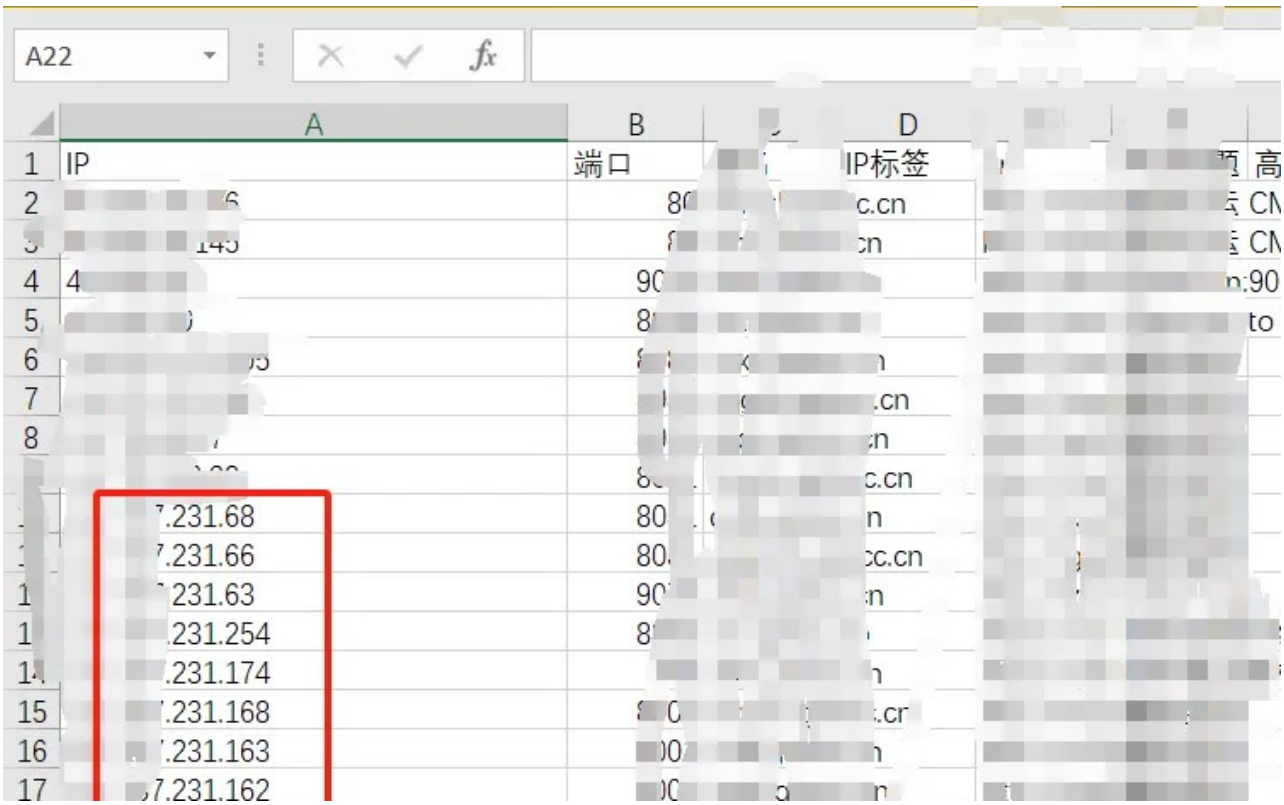
4.2.fofa 、hunter、Quake等空间搜索引擎

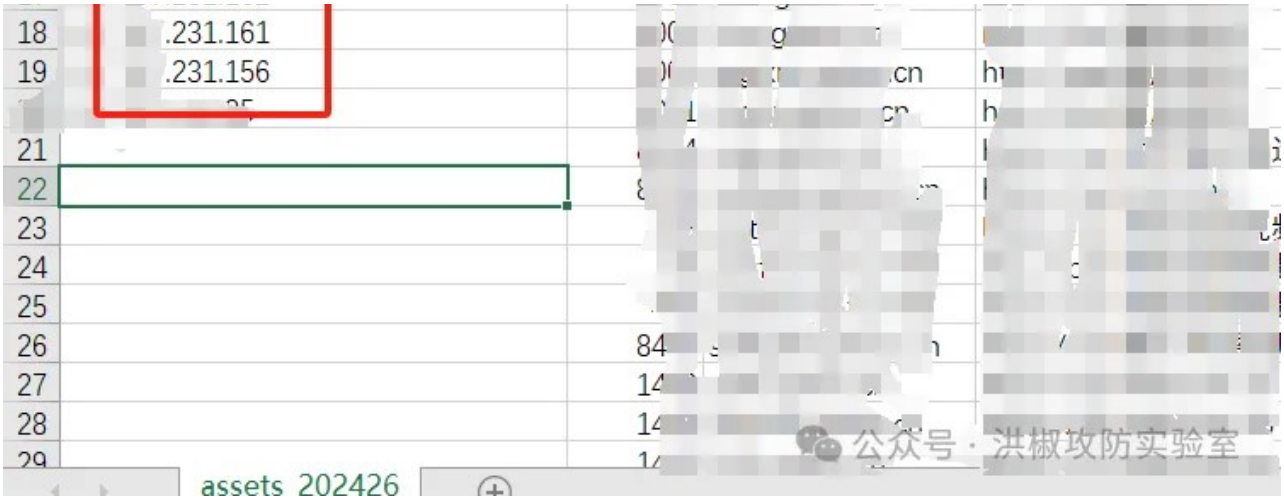
这个想必是大家一定会用到的，拿到资产根据关键词搞一波。例如:title="省某厅" 、icp.name="省某厅"等，这些都是简单的基本操作，下一步，可以对这些关键词进行衍生联想。

例如通过某省厅这个主单位联想可能存在的系统，然后将这些关键词继续代入空间搜索引擎中进行搜索。这里主要介绍hunter的icp.name功能，我比较喜欢用hunter发现IP地址，能快速的发现目标的主要资产和IP地址等信息。然后用Quake查单个IP(因为Quake探测单个IP的端口比hunter多) icp.name="XX省科技信息中心"



大家细心的很容易就发现上述资产，在同一个C段下，xx.xx.231.156-xx.xx.231.174，一般运营商给出口IP都是连着给的，小单位三五个，大单位几十个上百个都有可能。这个IP范围其实跨度蛮大的，而且资产会比较多，我一般直接用API的导出功能，然后使用word的数据去重+排序，就能得到一份大概的IP分布。





从图上面就能看到，从231.63-231.254，都有，证明这个单位的出口地址几乎占满了整个C段，这时候就可以直接用goby、xray等工具对C段进行扫描。

但是，很多单位并不会这么多出口IP，可能只有三五个；比如搜索引擎发现只有232.50 和232.53这俩IP的时候，我就会上下+5个IP地址，甚至10个，这能发现很多人发现不了的资产，直到发现这个IP不是该单位的时候，那就找到了这个单位的大概出口IP段，我一般用Quake一个个的看（Quake在单个IP资产发现方面吊打所有的搜索引擎），然后同时用goby、dddd等工具进行自动化扫描。

还有一点，在很多时候我们会发现我们用title、icp.name等语法搜出来的资产会有很多不相关的资产，所以我在针对某单位的攻击的时候，肯定是知道这个单位的地址在哪个省哪个市，打点就会把IP地址限定在某省。icp.name="省某厅"&&ip.province=="XX省"

但是在打一些北上广深的目标的时候，会发现一些大量的云资产，这时候就要做一些排除，防止打偏，hunter在这方面就做的非常人性化（各位师傅自行尝试）：

当然，云资产也不是不打，现在很多单位会把系统上云，从云上获取信息再攻击本地化的一些系统。

4.3.子域名

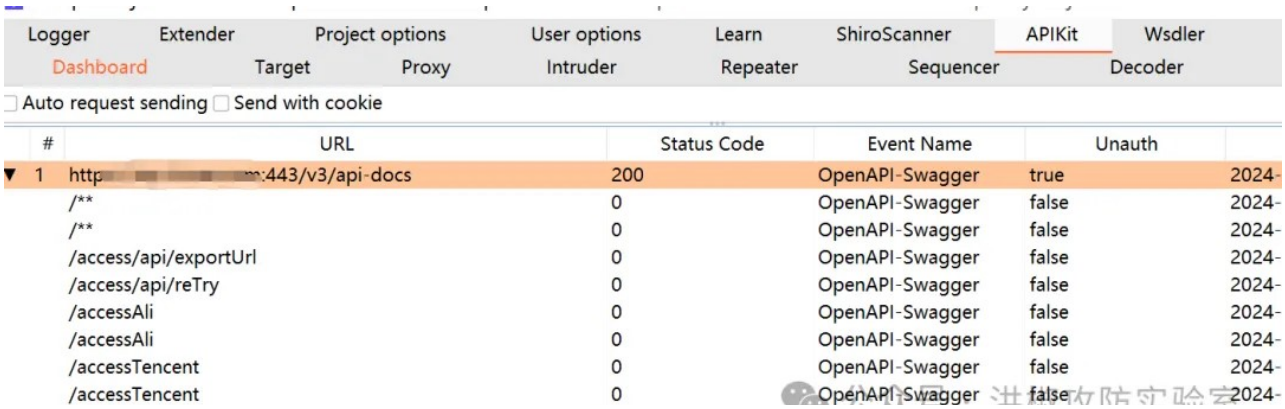
其实我个人感觉子域名爆破大部分是对于百度、爱奇艺这些互联网大厂的目标才会有一点作用，针对一些行业目标并不好使（因为域名太少了，至少交通行业我从来不爆破子域名。）需要爆破的话可以用SubFinder、挖掘机等等。

4.4.目录扫描

dirsearch是一个基于Python的工具，它的代码开源，使用简单且易于扩展。这是目前个人觉得最好的目录扫描工具，不接受反驳，反驳就是你对。下载地址：https://github.com/maurosoria/dirsearch请自行准备字典，GitHub上有很多师傅整理分享出来的。

4.5.APIkit插件

这个插件我推荐了好几次了，这是目前个人觉得最好的被动API接口扫描工具，burp导入就行，会自动扫描所有经过Burp的流量，时不时的点开看一下，说不定有惊喜。



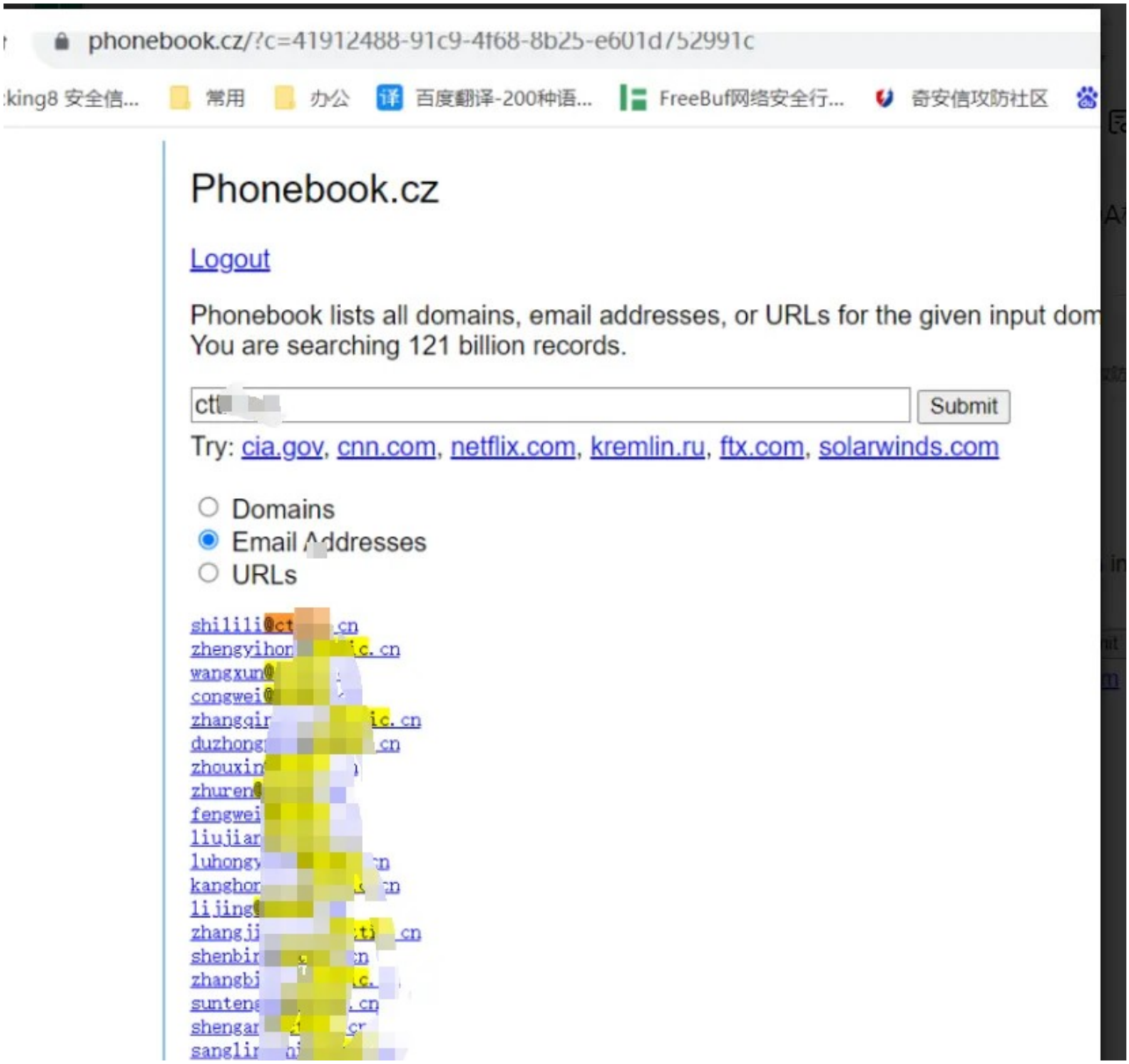
下载地址：https://github.com/API-Security/APIKit

4.6.小程序/公众号

现在小程序也成为了很重要的一个突破口，小程序的解密逆向可以看这篇文章：https://mp.weixin.qq.com/s/nLHEBRSAupAinpBHZG-Ebg。公众号一般都是集成WEB和小程序，复制链接到浏览器打开就行了，或者直接用的微信官方功能，没什么突破点。不做过多赘述。

4.7.邮箱

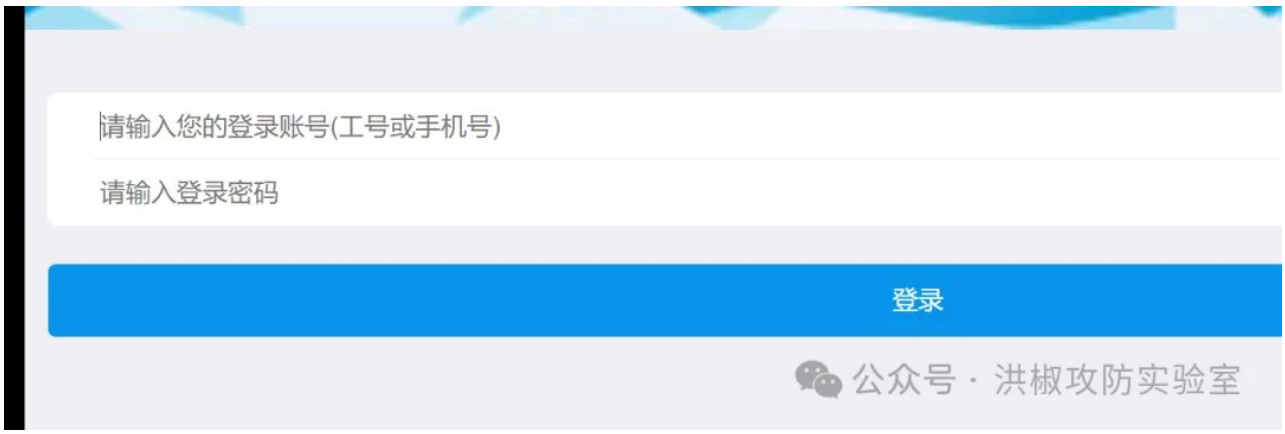
关于邮箱，很多是拿下一些OA系统账号得到通讯录得到邮箱，如果没有拿到OA权限，可以试试搜集邮箱https://phonebook.cz/logout



5.关于弱口令爆破

同一个系统，为什么别的队伍能突破，有的人突破不了？其实很多系统的账号其实并不是admin这些，而是单位的全写或者是简写，密码同理。例如：北京移动通信(举例) 它的用户名很有可能就是:Bjydtx、Bjyd、bjydtx、bjy*d*等等，那么密码就是Bjyd@123、Bjyd@666、Bjyd@2020、bjyd@2021、bjyd@2022等。

此外，其它用户名大概率可能是姓名简拼或者是全拼，我们也可以用它们作为字典进行用户名爆破。杨旭 yangxu yangx 张三 zhangsan zhangs ..... 还有如果提示工号的情况：



未知工号的情况：看单位大小，小单位可以爆破0000-9999。大单位可能是五位或者六位甚至更多，比如建行工行等等银行目标，工号是十位，但是也是有规律的，自增的。看目标情况，我一般爆破10000-11000 或者100000-110000。

很多单位工号是公开的，我们可以通过一些搜索语法去找该单位的工号，有的不是，甚至找不到，那我们就可以用社工的方法，拨打客服电话，询问客服人员的工号，然后得到位数或者规则，建立用户名字典。

如果存在用户名枚举的情况，用姓名字典先枚举出用户，然后再构造密码字典：例如：zhangsan 密码：zhangsan@123、zhangsan@2022 也可以用公司的密码字典，比如上面的Bjyd@123、Bjyd@666、Bjyd@2020、bjyd@2021、bjyd@2022等等。

总之，现在很多单位已经没有123456这种弱智口令了，更多的是规律口令，猜到了规律，你就有突破口。

5.总结

虽然信息搜集是一项很重要的工作，是开启后渗透的基础，但这项工作是体力活真的是不争的事实，因为它没有门槛，基本谁都能做，无非就是用工具对着一项项checklist不断的去尝试而已。因此通常意义上的快速打点，就是比谁先试完所有的checklist，虽然目前绝大部分工作都是由工 具来完成，整个项目呈一个半自动化的流程，但是仍然架不住资产量的庞大，一个信息收集熟练的人，无非也就是流水线的工人而已，对着巨量的资产不断的用工具筛选而已。

而一些高端打点技巧玩得好的人，例如电话钓鱼成功率很大的人，钓鱼邮件的撰写和钓鱼样本的开发做的很牛的人，在做这些事情之前，同样需要信息搜集，而能够玩高端技巧的人是不愿意来做信息搜集的，因为他们也是从小白阶段过来的，明白信息搜集这项繁重且技术含量低的工作完全可以找别人来做。

从公司层面上来讲，要快速打点，就要投入更多的人。从个人层面上来讲，要快速打点，要忍受枯燥的打点过程，然后提升自己的工具使用速度，最好自己能够进行二次开发，把一些半自动化的步骤连接起来，优化现有的步骤，从而进一步提升效率。

这里更大程度上，只是想把做一件事的动机以及如何权衡利弊做好一件事情的方法分享出来，大部分也是个人理解，难免会有错误，不足之处希望大家指正。