idc服务器溯源

攻击者个人服务器

- 查看是否存在备案信息
  - 查询到手机号
    - 去社工库查询相关人员信息
    - 去添加支付宝通过转账获取到部分人员名字
    - 去添加微信获取一些个人
    - 通过谷歌需要搜索手机号看能否获取到一些信息（比如可查询到Github等注册信息）
    - 去查询该手机号注册了那些网站（https://www.reg007.com/）
    - 去脉脉查询个人信息
    - 去抖音查询个人信息
    - 去微博查询个人信息
    - 以及一些其他社交平台都可尝试
  - 查询到邮箱
    - 去社工库查询个人信息，通过社工库的信息再去深度溯源，比如拿到了手机号及可通过手机号溯源的方式溯源
    - 通过谷歌语法去查询看能否获取到部分信息
    - 查看邮箱类型去深度溯源，比如是qq邮箱可以去添加qq再获取一定的信息
- 查看该IP下是否存在网站
  - 看网站信息是否有相关人员的信息
    - 有的是黑产网站可能会在网站中找到他的部分信息比如邮箱、电报号，则可通过获取的信息再去深度溯源
  - 看网站是否存在个人博客等信息
    - 可能他的博客就是用的这个用的这个服务器，那就能获取到他的部分个人信息
    - 可能会用公司的服务器，搞不好能碰到这个的红队，那找到公司了不是也一样了
- 查看是否存在历史解析
  - 使用网站回溯网站查询
    - 回溯网站(https://archive.org/web/)
    - 有的攻击人员在事先关闭他的网站，可以尝试利用网站回溯去查看原来网站的信息
- 端口扫描或漏扫一下
  - 尝试端口扫描一下
    - redis未授权漏洞尝试获取服务器权限去溯源
    - 一些端口尝试一些简单的爆破搞不好有收获
  - 漏扫一下也搞不好有收获但是遇到的少
- 去查看该服务器是在那家买的
  - 很多时候其他方法都没溯源到人的时候可以去查看该人员的服务器厂商是那家的，如果客户非要深究，通过报案去源头商家是可以获取人员信息的，但是国外就搞不了了

傀儡机

- 去查看该服务器下的网站，一般通过网站的类型很容易判断出是傀儡机的
  - 在无法反制的情况我们去获取傀儡机厂家的信息并在报告中写好溯源过程就行，因为不可能所有IP都能溯源到人
- 漏洞反制
  - 端口扫瞄
    - 通过一些端口弱口令或端口漏洞去获取服务器权限并对其深度溯源
  - 历史漏洞探测
    - 通过漏洞扫描器去探测是否存在漏洞，具体看当时情况而论

XMind | 试用模式