场景：

开始 xx 了，十几家单位啪的一下甩过来，然后一看，一堆金融单位的资产，心里一阵凉凉，然后尝试用 0day 打了一家，打是打进去了，但是内网横移的时候被流量设备抓到了，是真的设备多，session 掉了，入口点-1，0day-1。

应对上述情况，先从源头开始分析。

通常 xx 就那么几种手法，打点，钓鱼，0day 打点，然后进内网刷分。

攻击队经过规则分析，发现了内网可以刷 8k 分，然后换一套题刷这个规则。

基本现在的打法就是，外网找一个口子，然后内网刷满路径分，然后拜拜。

一般看需求，要求的多，有诚意，我就多刷几家。

没要求，没预算，而且项目经理还态度不行，不好意思，给你刷个两三千分顶天了，那么卖命干嘛，划划水不香吗？碰到有难度的目标想挑战一下除外。

那么由此引申出以下几个问题。

1、用什么方法在外网搞个口子出来成本最小，效率最高

2、搞哪家简单一些，捏个软柿子，不啃硬骨头

3、内网刷分，怎么刷最快，还不会被发现

4、什么时候提交报告最好，避免目标出局无法提交报告进而无法得分

问题一 撕口子

先说答案，钓鱼。

到了高防环境，基本只有两条路可走，0day/钓鱼。

0day 从外面收，要钱，自己挖，要时间成本，是一种综合来说成本较高的攻击手段。

钓鱼，可以拆分以下几个步骤。

-做免杀马

-写钓鱼文案

-写剧本

-剧本测试和推导以及突发情况应急

成本高吗？不高

学习钓鱼，有基础的人，最多最多一个月，钓鱼可以学得有模有样。

效果好吗？非常好

打点打不进去，直接钓鱼，有时候真的效果拔群。

因为钓鱼每家单位都可以用，而且每家单位有那么多人，只需要中一台机器，我就可以横向移动。

这里钓鱼不仅仅限于传统的邮件，也可以电话，微信，qq 等等等等。

以下放上社工钓鱼的祖师爷

凯文米特尼克

建议大家钓前拜一拜

如果有人不认识的话建议自行百度，反正我是买了他那本书《欺骗的艺术》
每天日常拜一拜祖师爷，然后翻两遍他的书，以表示我对祖师爷的 respect。

钓鱼的成功率为什么这么高？效果为何如此拔群？

因为钓鱼的本质其实就是骗，骗别人点一下我发过去的东西即可。

所以只要能够骗到别人，然后目标单位的机器能够出网，满足上述两个条件，就能够成功。

但是 web 系统不一样，更何况 xx 的时候，很多单位还喜欢拔网线，这搞个屁，有时候即便有 0day 都没法使用，机子下线了怎么打？

如果有人研究过电信诈骗的手法，就会了解，一般诈骗的人聊着聊着，会发个 app 过来，例如 ab 会议，需要你点击安装，然后进 app 中会议跟他聊。

其实就是个捆绑了 ab 会议的马，安装了之后，其实对方可以对手机的行为做一个整体的监控。

他们在安装 app 之后，还多了一个步骤，就是需要骗钱，也就是转账，费劲巴拉的。

但是成功率依然很高，每年被骗的人不计其数。

xx 行动中，钓鱼是这个的简化版本，只需要能够点击，不需要后续的转账环节，成功概率再次大大提升。

综上，整体打法的建模相当简单，这里拿 SWOT 来举例：

Strength：0day/钓鱼

Weakness：作战时间短，目标多，目标的 web 机器下线多。

Opportunity：每个人心里总有防护薄弱的地方，每个单位总有防护薄弱的人

Threaten：别的攻击队也在钓鱼会有干扰/目标单位不出网等

通过上述的比较分析，可以发现钓鱼的优势还是很明显的。

因此针对撕口子这块，策略建议做两手准备

其一是钓鱼，作为撕口子的主要技战法来使用

其二是 0day，在钓鱼也不好使的时候用

其三是 1day，在没事干的时候使用

其实解决了第一个撕口子的问题，后面的问题都好解决，只是时间问题而已。

软柿子：这个搞多了，看一眼名字就知道哪家是软柿子了，哈哈哈，无非就是非国有大型金融单位的其他单位，因为金融钱多，预算足，设备多，xx 的时候请来帮忙的人也多，就算打进去了，其实横移的时候也很容易被发现，毕竟人家请了那么多人，买了那么多设备钱也不是白花的。

刷分：xx 的时候时间那么紧，真的有人用 apt 的手法吗？就算有这个技术，你用了，但是别的攻击队也进去了，进去夸夸就是一顿扫，然后现在还只有个 webshell 的权限，上午刚拿到，下午因为别人进去扫，都还没来得及上 cs，目标直接关站。建议直接就 fscan 一把梭，管 tmd，路径分刷满赶紧把图截了，然后提交报告得分才是正事，靶标是不可能靶标的，这辈子不可能靶标的。

提交报告的时间：这里建议采用 0 信任法则，不要相信任何人。报告提交，你就可以明白，你的手法已经被公开了，具体谁知道了我不管，但我先不交。满了 8k 之后，我就在那苟着，继续刷下一家，直到接到消息了，说对应目标出局了，提交报告的时间是 xxxxxx，ok，

那我这个时候可以卡着点交了，但是有时候会遇到驳回，所以建议先写好，然后收到出局消息的时候马上提交，这样可以留出一个 buffer 给自己和团队做调整。如果打中的目标一直没有提交出局消息，建议比赛快结束的倒数第五天交了，时间不早也不晚，因为很多攻击队喜欢最后来交，但你想想，你如果是裁判，搞到最后，其实也精疲力竭，哪还有太多心思看报告，其实就想溜了，然后发现最后还有一大堆报告。那么这个时候，只要报告有一点点不清晰，那不好意思，直接驳回，看都懒得看下去。然后等结束了，收电脑了，你再改，再提交，谁来看报告？而且会认真看认真审吗？

以上基本是一点经验总结，没有具体的技战法，但是我觉得做一件事情，选择一定是比努力重要的。

这句话也可以理解为，战略一定是比战术重要的。

德国原来打俄罗斯，小规模的战术打得那么好，俄罗斯全线节节败退，但是因为初始的战略上出了问题，还是输了。

放眼全局，着重于最后的胜利才是根本。

做了详尽的情报分析之后，基于战略再来选择战术，才能更大程度提高成功的概率。

done