红队本身做事情，思路一定要对。

就好像写代码一样，如果思路不对，其实努力了再多，都是空谈，搞不好最后还要重写，反而浪费了大量的时间。

红队本身要想取得成绩，首先还是得结合市场来看。

目前由于各种hvv项目催生了大量市场需求，需求看似繁杂，其实对红队来讲，归根结底就是一条，就是实战攻防能力。

这个实战能力，指的是在该打的时候，能够去日穿对面的站，那就够了，其他不用多讲。

因为职业道路是可以观察前辈的脚步来进行推论的，看看自己走到了哪一步，基本都是有迹可循的，呈现一个客观事实。

现在的高端红队要么在乙方实战了多年技术够了跑到甲方去做攻防老大，相当于退役，因为很多甲方的攻防只是对内的攻防，没有对外的项目压力，不用时时刻刻保持竞技状态，同时依靠多年实战的经验也可以在甲方坐稳这个位置，要么就是依旧还在乙方的高端实验室待着，继续做深入的安全研究，要么就是自己出来单干了，在外面拉一只队伍，靠接项目赚钱，还有什么多样化的选择呢？基本没有了，技术的道路尽头就是这几个选项，就看自己怎么选了，因为技术能力栈被市场需求的点就那么几个。

乙方需要攻击队来打各种hvv从而根据名次获得各种政府/银行/机关的项目招标优势，然后服务人员进场，然后再卖设备，基本就靠这么三板斧来做盈利。

甲方需要攻击队来搞自己公司，给自己公司来挖漏洞，从而保证自己主体业务的安全，当然有的甲方还做对外的安全业务，例如tx，ali等大厂，那么攻击队思路也可以参考乙方，一回事。

自己在外面接项目，其实和乙方做一个概念，有时候也帮别人当打手，本质也是上面利益链中的一环，没啥大的区别。

说实话，我面试了这么多家公司，国内安全你说真正顶尖的人到底有多少，我觉得很少，就以我面试面过的公司，对方给我的直接感知来讲，360高攻算一个，深信服深蓝攻防实验室算一个，长亭上海那个攻防的实验室算一个，其他的可能也不是说水平不高，也有可能面试的时间短，聊的没那么深入，给我的感知没那么强烈。我不是说其他地方就没有高手，但我敢说上面我自己面过的这三家，给我面试的面试官肯定都是一线攻防的顶尖高手，当然，听口气基本都是实验室的老大，我是这么猜测的，至于准确度高不高我也不敢说死，也都是主观感受。

为什么我上面列的都是乙方的公司，甲方就没有高手了吗？

肯定有，但是相比在一线实战的乙方的这些攻防部门，我觉得量会要少一些。

因为甲方的人不一定懂实战，而且由于网络安全这个东西比较新，国内很多人接受+出策略还有很长的滞后性，这个滞后程度，其实不接触不知道，一接触是很吓人的，不是想象的接受的那么快，是接受的非常慢。

我其实觉得红队最优的路线应该是，毕业在国内乙方顶尖的攻防实验室沉淀几年，然后之后自己怎么选都无所谓，无论是继续在乙方做安全攻防/研究还是跳甲方去负责红队，还是出来单干，其实都好搞，因为乙方沉淀那么几年，可以把红队最重要的实战能力和实战框架搭建起来，这个是一个红队的核心。

我还见过一些人，走的是另一条路子，当然这种人不能算红队，他们是搞研究的，就是大学打CTF，然后毕业之后去研究性质的实验室，但不是攻防实验室，然后后续输出前沿漏洞挖掘研究成果等，这个路线也可以，因为也掌握了实实在在的技术，基础打得很牢固，但是和红队不是一个路子，红队是属于作战部门，他们这类相当于是研究部门，两个工种。

但是还有一些人的选择就有些糟糕了，就是一直干渗透测试，然后各个厂，不断地跳不同公司的渗透岗。

渗透岗是很基础的岗，渗透的进阶就是红队，红队虽然是以权限为主，但是你让他再回过头去干渗透，那分分钟上手，根本不在话下，本身单纯只是渗透的话，难度就没有那么大。

这种还是没什么意思，因为未来没有想象力啊，一直干渗透有啥意思呢？工资不涨，同时上限也很低。技术人员还是得不断进阶才有出路的。

那么走到了比如在甲方带红队/乙方实验室老大/自己单干，红队下一步职业生涯的拓展在哪呢？

我认为还是得比赛，比赛出战绩，然后通过战绩来扩大自己在行业中的知名度。

然后利用知名度去接项目盈利，具体什么项目因时而变，然后通过盈利体系积累通过技术创造的原始财富，然后再慢慢积累渠道，获得稳定客户，然后再洞察市场，找到市场痛点，就抓那么一两个痛点，做自己的稳定盈利产品出来，基本这条路就是这么个打法。

还有别的新意吗？能快速赚到钱吗？我觉得很难，肯定有，但我首先承认我找不到。

我的思想还是偏拙朴一点的，我觉得现在人人都想走快车道，都想抄捷径，那么这个时候，恰恰沉下心来，把自己的技术提升上去，把自己的战绩提升上去，然后不断的根据自己目前的情况来弥补缺陷，一点点往前走，不求走得有多么快，但是一定要走得稳，不要走一步退两步，扎扎实实的走就是了，这样在我看来或许是最快的道路，就一定是以稳固的基础慢慢往前推。

说完职业生涯方面的考量，这里再谈谈具体技术栈的考量。

还是根据实际作战需求来，打了这么多次攻防，需求其实很明显了，打点一定是排在最前面的东西。

可以列这么一个等式，打点成功 = 信息搜集成功 + 漏洞利用成功

因此就根据这个等式再往前推两步。

信息搜集，老生常谈，但是全部做到位的人真的不多。

这里我理解信息搜集的思路就是常规搜集+推陈出新的搜集方法积累。

常规搜集人人都会，无非就是各种扩散，ip+全端口+指纹识别等等这一套东西，但是这套东西里面还有很多可以优化的细节。

比如现在有的指纹识别系统是不是真的准确，这个需要自己去测，然后自己去调，根据目前的工具来做一些二开。

还有目录扫描，就是一个字典的问题，但是很多人就是默认字典在那里搞，没有自己实战中沉淀的字典来操作，这个也得调。

还有密码爆破字典也是，也需要调。

看似很多细节，好像很简单，但是就是这么简单的事情，很多人都忽略了，然后叫着打不到点，人家都用0day打点，我没有。

用心去优化，去观察，常规手法很多时候也是能够打到点的，关键就是看很多细节自己有没有去做调整，做优化。

常规搜集就这么些，还有推陈出新的方法，这些方法一方面靠自己研究，另一方面需要大量的去看别人的报告。

建议把先知，seebug等社区的相关外网打点文章都看一遍，看看别人是怎么找点的，然后光看印象还没那么深，得写读书笔记，自己脑中想象如果是自己遇到了这样的环境，是不是也能像别人一样打进去，还有没有别的方法。

广泛的阅读好处很大，很多时候我都是参考某些文章的思路，然后挪用了一些地方，然后在我自己打点的实战环境就打进去了。

这里信息搜集搞完，然后就是漏洞利用，利用也是一个路子，广泛的阅读文章，把他们各种绕waf的手法以及漏洞利用的骚方法都学习一遍，然后还得去做一些CTF的web题，提升思维广度，然后自己再带到实战中去琢磨，就会发现其实绕waf就那么几步，就那么几个套路，掌握了，会了自然就会了，没什么神秘的，无非就是多种思想的排列组合。

还有p牛的vulhub，不说全部刷一遍，常见漏洞是肯定要都过一遍的，一般的顺序就是常见漏洞+常见漏洞带waf的利用方法。

漏洞利用过程中有很多东西都是可以进行学习的，很多poc的变式有的时候也不仅仅是一种漏洞可以用，有些poc变式推广起来，威力还是很大的。

基本上面几个板块搞完，阅读个一两百篇文章+信息搜集技法强化训练+漏洞利用技法强化训练，大部分的外网打点工作都能够应付过去了。

然后就到了内网，也是一个路子，首先是阅读，看看别人怎么打的，然后暂时没有实战环境没关系，写读书笔记，遇到能实践的环境就实践一下，加深印象。

这里所有文章的阅读思路都是一样，阅读文章，最终还是要落到实处，就是能够应用，所谓学以致用，不然看再多都是空的。

读书笔记是在没有实战环境的条件下没有办法，没办法去实际的去应用实践一下，那么只能说去靠想象力模拟，模拟作者在当时遇到的情况，然后自己通过笔记的方法主动感悟转化一下，这样最大程度的吸收作者的思想。

如果单单就是读过去了，就这么过一遍，我敢说p用没有，一会就忘记了，最多在心里留个浅浅的印子，真正实战的时候也用不出来。

内网也是信息搜集+漏洞利用，思路都是一样，技法不同而已，而且如果时间有限，其实内网说简单也简单，说难也难。

难的话就是所有的环境叠加上，啥都有，啥设备都有，自然难。

简单的话就是进去fscan一把梭，看到有啥漏洞就打啥，根据扫描结果代理一挂，然后密码一抓，然后复用，真的很多情况就是这么打的，因为目标也没啥设备，这你说简单吗，也简单。

所以内网的学习不要抱太大压力，还是由浅入深，循序渐进，而且一般团队会有一个专门搞内网的，自己看看，如果搞不定，感觉不行，那就丢给他打就完事了。

反正在团队中的定位很重要，一定是要让自己弥补团队的空缺，找准自己在团队中的定位，发挥自己的最大价值。

然后就是钓鱼+免杀，免杀马这个东西学起来快，简单的免杀基本上就是实现一个shellcodeloader就行了，然后结合钓鱼套件一搞，就可以钓鱼了。

但是具体的钓鱼实施讲究很多，还要花心思去钻研一下，这个就不是一两天的功夫了，得花一段时间。

然后再就是代码审计，红队的代码审计思路依旧是沿用上述的思路，先看文章，然后复现，然后自己去实战。

这里如果要我排优先级的话，我就这么排

外网打点>内网渗透>代码审计 = 钓鱼免杀

上面是我根据自身情况定制的精力分配路线，因为我钓鱼免杀基本的项目都能应付，然后代码审计也是，简单的cms也能很快的审下来，那我的主要精力就还是分配在找点和做内网研究上，当然，不同的人的情况肯定不一样，因此需要根据自己的实际情况来调整。

然后就是这么不断的轮，看书，实战，复盘，研究，然后技术就得到了提升，没有什么蹊跷可言，就是笨功夫，做到后面做得快就是熟能生巧罢了。

总结一下，其实我就想强调红队的三个核心

1、职业生涯道路规划要抓住核心关键点来做提升

2、要下笨功夫，要多实践，多复盘，多思考

3、要有全局观，无论是在团队还是在公司还是项目上，要看清楚自己扮演的角色，然后做好自己的本分，然后在本分上再进行突破和超越

最后就是心态一定要好，不能浮躁，就慢慢的搞，慢慢的提升，很多事情在于坚持，不在于一时的爆发，这个世界的规律就是如此，跟着规律走，是能够取得成功的，前提是不能放弃。

Done