0x01 学生时代

其实我的整个学生阶段我认为都不具有有什么亮点，但还是简单带着说一下，虽然没有亮点，但是也具有一定的参考意义，因为和后来走上计算机这条路也有点关系。

学生时代基本就是玩过来的，读了一个不算特别好的大学，但是一本也是有的，也不能说太差，但是如果说拎出来说特别牛逼，我是没办法说的。

初中其实对电脑有点兴趣，买了谭浩强的C语言来看，也尝试过编译，但是看不懂，而且还被父母说，说不认真读书，看这些没用的，然后玩电脑被抓到还会被打。

高中的时候有参加信息竞赛的机会，但是成绩不好，父母和老师都不支持，又是在学校寄宿，平时没有接触电脑的机会，于是就没有竞赛机会了。

虽然客观来说没有很好的启蒙条件，但是也没事，还有大学。

但是大学的时间我也没抓住。

大学是我自己在瞎搞，读的就是计算机专业，但是没认真学，大一的时候稍微看了一些渗透的东西，但是兴趣还没上来，觉得不过如此。

那么又离开了压抑许久的环境，可想而知，玩乐天性释放，大量的时间就在打游戏。

然后学生时代就宣告结束。

如果问我有什么亮点，我很难去描述，因为的确没有什么突出的成就。

如果硬要问我这么长的时间，最大的收获是什么，我觉得就是骗人，因为要想一直玩，但是又想蒙过家里人，蒙过老师，就需要伴随大量的谎言，家人和老师都不傻，所以这个事情不算容易，反复的实战和推敲，就锻造了高超的骗术，至于骗术的意义，在后续会提到。

0x02 工作生涯

和大多数入行的人一样，我也是从安服干起的。

安服的事情很简单，当时面试之前就稍微浏览了一下相关的内容，然后看了看面经，刷了刷对应的面试题，然后就过了。

不是我聪明，是确实难度不大，能混，仅此而已。

在我工作的前两年都在干安服，两年的安服生涯回忆起来带给我的好处也有，我分别来阐述。

第一年给我的感悟就是知道这个行业大概知道需要干什么，然后平时做了一些简单的漏洞测试，一些复现，积累了一点点技术的薄底子，仅此而已，其实第一年还是在玩，因为工作了拥有了金钱自由，很多以前读书受限制的东西都可以自己赚钱去玩，比如旅游什么的，所以继续解放，心思没有放在技术上。

第二年，在老家玩腻了，想出来看看，就来了上海，同样也是找了一份安服性质的工作，具体的title不提，反正性质和安服差不多，就是测应用。

在第二年这一阶段，见识的面更广了，因为应用包含小程序，app，以及各种站，然后也知道了甲方SDL测试的流程，然后同时也有一些攻防的属性存在，算是技术有了一个基本框架，但是技术说有什么沉淀，我是觉得完全扯淡的，我认为当时我的技术是非常垃圾的。

两年结束，第三年就去了实验室工作，也是我的第三份工作。

可能有人觉得这个跨度很大，其实我也觉得，安服仔混了两年，实验室怎么会要我？这个就需要跟前面的骗术扯上强连接了。

我虽然技术不好，但是我洞察力和短期记忆能力还行，就是能够从一次面试中提炼出要点，然后补上，然后下一次以面试官想要的表达传递过去。

然后就算不太会的知识点，现学现卖，可能是昨天刚看的，我会一连串的说出来，给面试官造成一种假象“他其实很懂这块，就不用深入问了”。

然后语气由于长期骗人，已经养成了平稳有力的语调，同时对人心理活动的洞察也能够通过对方的语气判断出来， 即便是在电话面试中看不到对方表情，也能判断个八九不离十，那么经过多方技巧加持，综合利用一下，就容易蒙混过关。

至于其他的技术还有话术细节还有很多，基本都是实战总结出来的骗人的东西，也就是现在和钓鱼一起发扬光大的社工技术，在面试中用了很多。

当然也不是一次成功的。

当时记得很清楚，面了三家，都没过，最后面到这一家，把前三家暴露的缺陷全部修补上，加上我提炼出来的面试官想听的东西，然后过了第四家的实验室的面试，然后入职了。

在这家公司待了两个实验室，一个是专门做漏洞研究以及0day跟进分析的实验室，一个是专门做攻防的实验室，然后总共待了一年多。

第三份工作给我的帮助很大，主要体现在以下几点

1.技术框架系统化

因为在公司内部的两个实验室都待过，实际上代码审计&漏洞利用&产品维护&工具编写&安全研究都有接触到了，我虽然基础差，但是遇到了问题还是愿意去学习的，再加上安全这个模块本身不难，所以稍微够一够，也能够混过去，同时遇到的两个leader都很不错，一个主攻CVE&漏洞挖掘，一个主攻实战，圈内都是名气++的，通过跟leader还有实验室的同事学习，帮助我搭建了较为完善的技术框架。

2.实战化

去到公司的第二个攻防实验室之后，做了大量的攻防项目，给了技术实践的空间，不懂的问题实战暴露过一次之后，事后会大家一起复盘总结，得到解决问题的方法，然后第二次项目持续演变改进，逐步逐步的，技术就得到了稳步提升，并且养成了复盘的习惯。

3.思维模式提升

思维模式指的是思考问题的方法，以前是没有怎么想过的。和优秀的人同行，其实会受到别人的影响，会汲取别人的优秀的思维方法，然后提炼成为自己的。实验室的小伙伴针对技术大多都有自己独到的见解，那么得出见解的过程就是他的思维模式，不断模仿这些过程，然后自己在实战中加以应用，然后再适配自身的特性定制化，就逐步形成了自己的思维模式，好用并且兼容性强，还能够随时扩充新的好模式，就好像现在扫描器通过yml文件扩充新的poc一样。

4.规划清晰化

在这段时间认真的思考了自己未来的技术路线规划，这是以前从来没有过的。

安全技术对我来讲没有那么玄乎，就好像打游戏一样，就是不那么讨厌，然后上手玩玩这种感觉。

如果要扯什么非常喜欢，然后极其热情的去做技术，抑或是冥冥之中感觉自己天生就是干这行的，我认为纯属扯淡。

扯到极其热情，我突然想到初中的时候打游戏，那时候寒暑假都有补习班要上，很烦，耽误我去网吧打游戏的时间，因此我特别讨厌学习。

那时候流行一个游戏就是疯狂赛车，盛大出品的，我真的是极其热情的在玩这个游戏，上课的时候脑子里都在想车要走哪条线会快一些，并且当时有个地图叫雪邦，是个较难的图，有很多地方需要用到压车的技巧，当时数学课脑子里就在盘线，然后一下课就跑回去实践。

其实我觉得这个算极其热情，加专注，因为真的心无旁骛。

不过后来玩游戏就很少有这种状态了，包括做事也是，我理解就是，从小我的爱好就没有得到满足过，这种专注度没有得到培养，因此慢慢的就流失了。

但是在实验室这段时间好像让我找回来一些以前的感觉，于是我开始规划了一下我自己的未来，规划的结果也很简单，就是专注的做技术。

可能从接触到喜欢也需要一个过程，后来不断深入研究的过程中，慢慢的自己也更加喜欢做安全这一行了，可谓干一行爱一行（笑）。

因为随着不断理解问题的本质，其实发现还是很好玩的，不断的去研究突破，解决问题后，内心的喜悦也会逐步增加，这个和金钱无关，正如当初打游戏过关或者刷新记录会感到兴奋一样，这和盈利无关。

到了这个状态之后，会发现其实公司给的要求都是很低的，他只有业务要求，实际上自己如果喜欢，钻研起来兴趣大的话，做一个点会深得多，而且会不由自主的去研究和探索。

那么为什么会离职呢？有两方面原因

其一是觉得视角不透明，因为我们总是作为乙方来做项目，没有攻防的交互性。也就是打完这一波，其实都是黑盒在打，打完之后甲方会怎么修复，甲方真正的网络拓扑是什么样，甲方内部究竟是怎么来做防御的，他们是怎么看到我们入侵痕迹的等等一系列问题都不知道，这些视角很重要，但是又是是乙方缺失的，也就是说，乙方不具备全局视角，更多的还是黑盒视角，慢慢做到后期，就会迎来边际递减，收益会逐步变小，这个时候就会想要解决视角盲区带来的问题。

其二就是钱的问题，我虽然技术不行，但是谈薪还行，每一次谈薪，基本都是上一份工资的double，同样也是骗术扎实的功劳。实验室虽然好，但是我的节奏基本是一年左右换一次工作，每换一次double一次，公司内部涨薪途径肯定无法满足我这么夸张的涨薪幅度，只能寻求外部的其他公司接盘，再加上在实验室沉淀了这么久，技术远比原来扎实，信心也更足了，因此想着继续跳。

于是在22年初离职了，一边刷大甲方面试一边自己做项目。

面试的过程还是大差不差，刚开始因为乙方和甲方面试的东西不太一样，因此前几家用来练手的公司肯定是失败的。

然后还是老套路，总结完技术细节，然后调整，然后后面面试的公司就都过了，待遇也达到了预期。

然后做项目的过程中，也收获了很多，比如如何和别人去谈项目，项目全流程闭环，例如售前、poc测试、技术交付、售后、回款等等系列流程自己都有亲身参与，也知道了不同客户的需求是什么，怎么交付才能达到预期等等。

最关键的一点是，思维模式进一步进化，完成了从单点打工到商业化思维模式的一个转变，正如当初刚刚进入实验室完成技术框架搭建一样，这里是完成技术商业化的框架搭建。

搭建到什么程度呢，我在22年面boss直聘的时候，当时那边招蓝军负责人，已经过了两轮技术面+一轮hr面了，然后最后到了CTO面试，CTO问我未来的职业生涯规划，我就很老实的说

”未来还是想创业的，然后我本来不准备说的，你问了我，我不能骗人，我还是得说，因为如果你们要招一个稳定的人，我干一两年跑了，到时候你们会骂我“

CTO就笑了，然后说我很坦诚，然后最后没给我过。

虽然没过，但是其实内心的框架是做起来了的，也不后悔，未来的确打算逐步过渡到自己全职做项目这样一个状态，坦诚对大家都有好处。

同理还有面华为的时候，三轮技术都过了，第四轮是事业部负责人面试我，聊了一会，最后谈到我的职业生涯状态，问我

”你为什么离职之后会选择在外面挂靠一个公司做项目呢？你还这么年轻，为什么不上班呢？“

其实华为的人都还蛮优秀的，无论谈吐还是技术，从一面到终面的那几个技术官都是很不错的，提问礼貌，同时问的问题也富有针对性。

然而如果和领导理念不一样，其实很容易闹不对，尤其是华为这样的企业，发展已经很久了，体制较为固化。

加上我又是一个不太喜欢别人管我的人，从小也很叛逆。

三国演义有云：”大丈夫生居天地间，岂能郁郁久居人下“。

水浒传中有个情节，林冲到了梁山泊之后，当时首领还不是晁盖，是王伦。

王伦小肚鸡肠，不能容人，林冲在他手下待着受了一肚子气，后来找到机会，联合几个兄弟就把他杀了，然后拥护能容人对兄弟有义气的晁盖作为新首领。

也不是说一定会发生什么事，只是有些东西需要提前设想到。

我从来也没想着在别人手下一直干，就算取而代之，也意义不大，因为就算在公司当部门领导，头上还是有人在管我。

那么这里就明确了，各个公司对我的意义就是学习，学习我所缺失的东西，然后最后我自己这边来做整合，然后整合到位了就可以自立山头。

于是最后选了一家自由度相对较高的甲方，在这边整合我缺失的甲方攻防视角，一边防守方同学连动，看看他们是怎么做策略来修我的漏洞的，一边自己学习企业纵深防御体系，研究设备是怎么组合布防的，从而在做攻击的时候更具针对性。

这也就是我的第四份工作，在甲方负责红队这块。

因为目的很明确，同时自身各方面基础框架的搭建已经在实验室完成了，在甲方就相当于往里面填东西，这个就比较简单了。

另外甲方这边还附赠了一些管理的职能，我觉得有必要说一下。

我是认为人本身是无法培养的，就像石头一样，是翡翠，即便未经雕琢，它本身也是翡翠原石，一块普通的鹅卵石再怎么雕琢，也不可能变成翡翠，就是这么个道理。

人和人之间的差别，就像石头一样，虽然同样都是石头，其实是属性的差别，不是培养的差别，这个需要做区分。

如果是优秀的人，其实不太需要管理，他有自己的主观能动性，只需要提出目标即可，他就会想法设法完成。

如果继续下沉，可能就会各有各的差，就需要所谓的”管理“。

说好听点是管理，不好听点就是监督，需要人盯着才能完成任务，同时完成质量还堪忧。

因此面试本身至关重要，招一个初始就是优秀的人比什么都强，进来只要稍微交代几句即可。

然后再回归技术这条线，理论上来说一个安全行业的通才是完全可能的，就是从审计到利用之类的东西都会。

首先就是业内是有这样的人的，我也见过。

再就是把分离度降下来，从原子级别出发，安全这么多东西，看似繁杂，其实很多点都是可以以点带面的去学习的，学会了一个，就能打一片，然后再进行原子级别的排列组合，形成原子组，然后再拿这些组来再次组合，最后形成知识体系。

安全分裂到原子级别就是代码和漏洞逻辑，掌握了一些基本的东西，然后就不用记忆那么多了，用的时候可以自己去递推，就像数学公式一样，根据基本的定理去递推，通过这种方法，其实最后也可以掌握很大一个面，成为一个所谓的"通才"，这个从理论上是可行的，从时间上，假设我这辈子只做安全这件事，那也是可行的，因为安全这件事绝不需要花一辈子时间来达到专精。

成为通才，然后再去做企业，然后再去招自己想要的人，自己心里才有谱。

就是可能研究的面没有单方面专精的人那样深，但是如果完全不懂，那就只能听凭别人忽悠了，这不行，尤其是对于技术出身的人来说。

0x03 未来规划

未来还是慢慢往自己创业这个方向靠吧，现在理了一下，在目前这家甲方一旦学习完毕之后，就还缺一些东西需要学习。

1.大公司的管理模式

这个得去大公司当一个管理才能学到。

在当前这家甲方把甲方安全视角吃透之后，再加上以前的乙方视角，技术这块就相对健全了，因为有完善的框架，后期技术就算有差也可以自己针对性的去补。

这个时候就可以再迁移到一家成功的大公司然后学习他们的管理模式。

2.商业经验&思维强化

目前做项目只能说初步具备了一些商业思维的框架和经验，进一步强化还需要大量实战训练，这一点还没有太想明白怎么操作比较好，或许是自己单干然后不断的去从项目实战中总结，或者是到大公司的前端市场部门去学习，学习完毕之后对于商业流程的把控心里就有了底。

0x04 总结

总而言之，我觉得我的经历其实有蛮大的参考价值，因为不具备特异性，不是说一路名校过来，一路拿奖过来，我觉得这种经历是没什么好说的，如果最后没有做成才是离谱，因为都努力这么多年了。

我和绝大多数人一样，贪玩、然后整个学生生涯不务正业，一直到工作两年之后才迎来转折点，应该是这个转折的结果不是必然结果，是走了狗屎运。

没有实验室那段经历，估计也继续混过去了，也不会想提升，混几年也就回老家歇逼了。

可能是实验室那段时间，大家心中都有研究技术的热情，逐步点燃了我，让我找到了原来打游戏的时候的那种热情吧。

每个人心里，应该也有一个这样的自己吧，希望大家都能找到他。

Done