//20230525 补更

//增加多角度思考问题策略

其实感觉个人每段时间都会有些变化，看问题的角度和方式都会更加客观。

找工作这里补充一下，其实我们要追求一个 offer，一个结果。

之前我的角度总是站在一个对方的对立面来思考，比如我是求职者，我和 hr 去 battle，和面试官去 battle，这样是不对的。

因为我的目的是要一份自己称心如意的好工作，要一份好薪水，仅此而已。

面试的过程不是一个对抗模型，是一个筛选和互相了解的模型，了解过了，大家觉得 ok，然后就签合同。

本质是追求一个双赢的结果，面试者找到好工作，然后企业找到好人才。

那么用对抗模型来做这件事情，势必要出事情，毕竟不是一锤子买卖，过去还是要上班的，要一起协同工作的，是作为团队来联动的。

关系搞僵了，对大家都没有好处。

因此这里需要采用一个规划原则。

就是把能够争取到的力量都规划到自己这边来。

hr 砍薪水不是因为他们傻逼，而是因为他们也有绩效，也有 kpi 来完成，你要得那么高，搞了人家的绩效，人家肯定不乐意。

面试官有时候问问题深度一点，难一点，不是因为人家要刁难你，而是因为他想看看你技术的底子怎么样，为自己团队招到更合适的人，毕竟以后要一起干活，谁也不想和傻逼一起干活，仅此而已。

为什么我的想法会发生变化，因为我现在也在带团队招人，真的大无语。

角色身份改变之后，以前不能理解的事情都能理解了，其实都很正常，大家的立场不同罢了。

但是追求双赢这一点是肯定没有错的，这里是面经，我依旧站在对面试者有利的角度来讨论这件事情。

面试者在谈薪的时候，如果要得很高，那么这件事情是需要人去推动的，要走薪水审批流程的。

这个时候，是业务部门的人+hr 一起来推动这件事情。

如果把人得罪了，他们不愿意推，一个 reject 就丢过来了。

因此更成熟的面试策略主打的还是一个和谐共赢，hr 砍薪，你一开始要高一点，让她砍个几千又何妨，她心理上也舒服一些，意思大家各退一步开阔天空。

如果不是真的有必要，不要轻易得罪人。

我是一个脾气很差的人，我得罪的人一定比绝大多数人都多，说这个我是很有发言权的。

带来的结果就是处处树敌，要找人帮忙的时候，任何事情都很难推动。

主观上人家看到我就很烦了，还说推事情，直接一句什么什么不合规，什么什么流程没走完，要等，就合理的拒绝了。

因此处事圆滑并不是一种个人性质上的改变，可以理解为一种技巧，bypass 别人心理上的 waf，毕竟谁也不喜欢一个整天臭脸的人，大家都喜欢每天笑嘻嘻的人，帮个忙基本上主观层面也愿意帮了。

遇到了原则问题，该锐利的时候，还是锐利起来。

能和稀泥的问题，就不要太较真，多想想别人为什么这样做，如何 bypass 才是更成熟的方法，就像我们研究 waf，研究 hids，研究 edr 的策略一样。

要把他们想象成固有的东西，研究他们的性质，最后找到解决方法，因为别人的规则已经写好了，我们没法改，我们能改变的只有自己的策略。

//20221111 补更

//增加写在前面的话

在找工作的时候，我觉得有一点是比所谓薪资待遇还有其他福利啥更重要的，就是自己是否能够融入这个团队。

一般来说，面试时候的面试官就是以后的同事和领导，和他们聊天基本就能够获得很多想要的东西。

面试的时候，除开技术和团队之外，还有一个很重要的东西需要观察，就是领导的心胸。

先说结论，很简单，如果一个面试者的能力超过了技术部门的直系领导，那不好意思，面试必然是过不了的，还是那个很简单的道理，一山不容二虎。

招一个能力过强的人进去，大家又都是吃技术这碗饭的，我是傻逼，我不想赚钱了，我想找个牛逼的人把我顶掉，有这个道理吗？

再一个除开面试之外的东西，就是表述时候的语气和态度。

假如我是面试官，然后我面试一个小伙子，对面技术还行，但是说话还有点吊吊的，好像不太好管的样子，你说我会要这样的人吗，我必然不会，肯定直接挂掉。

还有一个就是 hr 的态度，一般技术面试完之后，hr 会来谈薪水。

一般的话术无非就是压薪水，最傻逼的一种，会问之前薪资和之前的之前的薪资，然后说“你薪资增长太快了，不行啊，我们给到 xx 钱已经是极限了，你要的 xx 钱是肯定给不到的注意，一旦 hr 用了这种什么肯定，一定之类的词来谈薪，就代表之前的面试官已经输出了态度给了 hr，hr 只是针对之前的态度来负责协商薪水的，她不起决定作用。

兄弟，听我一句，如果不是太弱真的没得选，直接 drop 掉，拜拜。

一个很简单的道理，去之前，都开始扣扣嗖嗖了，leader 态度也不咋地，指望真正加入了之后拥有过更好的体验吗？那必然不可能的。

找工作其实就是谈生意，我把自己用一个合适的价格卖出去，找一个合适的买家，无非就是这个道理。

谈生意当然要协商价格，因此并发找多个买家是必然的选择，公司也是一样，他不可能只面试一个候选人就定了，一定是不断的面试，然后找到适合自己的人，大家都是双向选择，选到合适的，就找到了当前的最优解，不存在说什么非谁不可，不存在的。

钱多就去，钱少就换一家，当然，谈价格要建立在自身实力的基础上，不然没人接盘。

再谈几个恶心人的挂人办法

1、面试完后，延期一周，然后发个拒信（时间拖延法）

2、技术面试都搞定了，然后薪资上故意用一个低薪水卡人，让你自己放弃（自主放弃法）

现在行情不太好，说是都在裁员，这个时候就开始拼眼界了。

目前确实处于经济大萧条时期，但是经济大萧条就不能赚钱了吗，我看未必，无非就是难度增大而已。

眼界的重要性体现在选择行业上，更简单一点来说，首先就是不要选大家都选的行业，具体原因就不细说了。

再一个，就是选择在既定的行业深耕，充实自己的竞争力，换维度竞争。

一旦维度提升了，那么竞争就不在一个层面，就会能够在恶劣的环境中也赚到钱。

这里还可以换个角度来理解，如果一个行业一直很牛逼，那么赚到了钱，到底是因为行业牛逼，还是赚钱的那个人牛逼呢，换个人，是不是别人遇到了那个机会，也可以呢？

真正的高手，一定是在恶劣的环境中，也能够保持相当的盈利能力的，也就是所谓打硬仗，不取巧，同时能打胜仗的能力。

沧海横流，方显英雄本色，这句话映射了一个很磅礴的意向。
如果当不了英雄，那么当个土匪也是可以的，把狠戾刻在骨子里，然后敢打敢拼，而且现在的情形又不是说差到饿殍遍野，族内互食的情况。
信心从来都不是别人给的，很多人看政策，看经济风向来获取信心，那只能说一句：
“道友，道心不坚，放弃修仙吧。世人随波逐流，生老病死听天由命，如浮萍一般在大潮中摆荡一生。修仙乃逆天而行，凶险万分，道友心智不坚，恐极易走火入魔，堕入万丈深渊”
转化一下，修仙的本质就是高人一等，拥有普通人没有的东西，和赚钱，当官等一系列行为并无本质上的任何区别。
想上升，但心智不坚，恐怕事还没成，已经被自身的情绪反噬了（心魔，哈哈哈）。
----------我是分割线----------
---2022 面试题部分---
主要提供两个方向，一个是漏洞挖掘，一个是红队。
面了之后，直观感受是，面试也是有套路可言的。

这里的套路指的不是所谓的出题套路，而是涉及的技术栈，都是大同小益的，无非就是那么几样，java，域为主体，其他为辅助。

虽然技术栈不变，但是面试的问题每一年都会略有改变，因为安全技术在进步，每一年面试问的东西，或多或少都会和当年出来的新技术有关系，而目前更多的会涉及到云这一块。
所以搞安全，一定要与时俱进。

市场要求，本质上还是底线要求，他要求你能够胜任当前岗位，这个要求已经很基本了。
对自己的要求应该还需要拔高，更多的应该是因为兴趣就某个问题进行深入钻研，然后完成各种各样的挑战，这样玩下来才更有乐趣。
其实不太需要思考钱的问题。
技术到位了，公司开高薪是水到渠成的事情。
越过过程去想结果，是很难有所收获的。

这里先对各家厂商的面试做个总结：
一 java 很重要
二 域很重要
三 如果 java 和域都过关，basement 的技术栈已经过关了，后续的就是锦上添花，在给你 offer 的基础上加钱。

Java 主要涉及新漏洞和老漏洞的原理，利用，绕 waf 利用。
域主要涉及新漏洞和老漏洞的原理，利用，绕 edr 利用。

至于红队方向，有的会问 cs 隐藏，cs 特征修改，这个也是必会的。
还有免杀，会了更好，不会也没事，如果 java 和域这块过关的话。

漏洞挖掘方向，需要能产出漏洞。
那么会问的很细，例如 cc 链某条链条的原理，为什么打了 patch 就不行了？为什么这样绕过又可以了？为什么后续 patch 的 patch 又能修复了？
例如反序列化，为什么我用这条链就行，另一条链就不行了，不行的原因在哪？写内存马用

哪条链条？Javaagent 了解过吗？如何动态修改字节码？内存马的持久化研究过吗？
漏洞挖掘，毕竟是单点的代码方向，可以理解问问题的深度。

因此可以这么区分
合格红队=java 利用 ok+懂一些原理+能挖一些简单的洞+内网 ok
合格审计=挖洞 ok+懂一些利用

后面是问的问题和对应价格参考，没写就代表我不知道。
数据不保真，仅供参考，真实度自行判断。
有些重复的问题就不一一写出来了。

//漏洞挖掘方向
shopee（30k+)
1、和信息安全相关的返回 response 头（https://www.cnblogs.com/yungyu16/p/13333909.html）
2、linux 常见命令
3、docker 常见命令
4、jwt 是什么
5、weblogic 反序列化原理（有一个 xml 反序列化漏洞 还有后台文件上传 还有二次 urldecode 权限绕过）
6、java 代码审计 exec 命令执行的相关利用 前面拼了一段 然后调用 lang.runtime.exec("fuck" + a) 这里可以利用吗 （不行 因为根据 exec 的方法 这里不能识别执行）
7、内存马相关原理
8、shiro 反序列化漏洞利用的时候 由于 waf 过长 被 ban 了 怎么解决这个问题（如果是 waf 拦截 可以尝试更换 http 头 如果是 tomcat 头过长 可以在 cookie 写一个 loader 然后 shellcode 写到 body 里）
9、内存马扫描原理 如何检测内存马
10、java 代码审计反序列化原理(输入的恶意类被识别 解析了)
11、ysoserial 原理 commoncollections 利用链的原理 (cc1 最后 invoke 反射加载输入的方法 cc2 cc3 等等大同小异)
12、linux 全盘查找文件命令(find / -name fucku)
13、docker run 的常用命令(docker run -it centos -p --name -d)
14、java 反序列化 php 反序列化 python 反序列化的区别和相同点(java 反序列化需要利用链 php 反序列化也需要利用链 python 反序列化不需要利用链 有一个__reduce__可以自己构造命令执行)
15、linux 全盘搜索含有某个字符的文件/linux 全盘搜索叫某个名字的文件(grep -rl 'abc' /)(find -name / fucku)

大疆（30k+)
1、mybatis 的 sql 注入审计如何去审
2、一个站，只有命令执行权限，没有回显，也不出网，怎么后续深入利用（发散）

深信服(30k+)
1、宽字节注入原理，是只有 gbk 编码的才存在宽字节注入吗？
2、php 反序列化原理

3、内网一台机器，只有一个 mssql 的服务账户权限，如何进行后续的利用
4、rsa 算法原理/aes 算法原理
5、一台机器不能出网，如何把一个 exe 文件放到对应的目标机器上去（dmz 区）

华为
1、log4j 如何绕过 trustcodebase
2、Springboot+shiro 环境如何进行渗透
3、实战中如何判断 fastjson 的版本
4、Fastjson 文件读写 gadget 是哪条，原理是什么
5、内存马类型，如何检测
6、给一个后台登录框有什么利用思路
7、Spring4shell 原理&检测&利用
8、安卓系统如何进行 rce，有什么思路
9、给一个移动端的 app，已知服务端是 cloud 环境，有什么思路利用

//红队&&企业蓝军方向
360 面试题（以下都是同一场面试提的问题，两个面试官，一个代审一个红队，时长接近两小时）

面试过程中一个很有意思的事情
在面试过程中发现 360 问问题的红队大哥是我学长，大哥一开始先问我
“你在学校有没有参加过一些社团“
”有参加 但主要是玩票为主 安全也玩一些”
“我看你跟我一个学校的，但是我没见过你啊？”
“啊？您是哪一届的？
”1x 届
“噢噢噢噢 我比你小两届 那学长你认识 xx 嘛
”xx 啊 认识 搞逆向的
“噢噢 那是我隔壁班的
”噢哈哈 行 你等一下 等另一个面试官接进来
然后学弟并没有受到厚待，以下就是火力全开的问问题

1、shiro 如何绕 waf
2、weblogic 如果在打站的时候，一旦遇到了 waf，第一个 payload 发过去，直接被拦截了，ip 也被 ban 了，如何进行下一步操作
3、jboss 反序列化原理
4、weblogic 反序列化原理，随便说一个漏洞，然后说触发原理
5、fastjson 怎么判断是不是有漏洞，原理是什么
6、fastjson 判断漏洞回显是怎么判断的，是用 dns 做回显还是其他的协议做，为什么
7、fastjson 高版本，无回显的情况，如何进行绕过，为什么可以这样绕过
8、代码审计，做过哪些，主流的代码审计 java 框架请简述
9、泛微，致远，用友这三套系统代码框架简述
10、泛微的前台漏洞触发和后台漏洞触发，如何通用性的挖泛微的洞，泛微能反序列化吗，怎么挖

11、php 代码审计如果审计到了一个文件下载漏洞，如何深入的去利用？
12、php 里面的 disable_function 如何去进行绕过，为什么可以绕过，原理是什么
13、假如说，在攻防的时候，控下来一台机器，但是只是一台云主机，没有连接内网，然后也没有云内网，请问怎么深入的对这台云主机进行利用？
14、redis 怎么去做攻击，主从复制利用条件，为什么主从复制可以做到拿 shell，原理是什么，主从复制会影响业务吗，主从复制的原理是什么？
15、becl 利用链使用条件，原理，代码跟过底层没有，怎么调用的？
16、假如我攻击了一台 17010 的机器，然后机器被打重启了，然后重启成功后，机器又打成功了，但是无法抓到密码，为什么无法抓到，这种情况怎么解决这个问题？
17、内网我现在在域外有一台工作组机器的权限，但是没有域用户，横向也不能通过漏洞打到一台域用户的权限，但是我知道一定有域，请问这种情况怎么进入域中找到域控？
18、jboss 反序列化漏洞原理
19、内网拿到了一台 mssql 机器的权限，但是主机上有 360，一开 xpcmdshell 就被拦截了，执行命令的权限都没有，这种情况怎么进行绕过。
20、什么是 mssql 的存储过程，本质是什么？为什么存储过程可以执行命令？
21、如果想通过 mssql 上传文件，需要开启哪个存储过程的权限？
22、内网文件 exe 落地怎么去做，用什么命令去执行来落地，如果目标主机不出网怎么办？
23、内网域渗透中，利用 ntlm relay 配合 adcs 这个漏洞的情况，需要什么利用条件，responder 这台主机开在哪台机器上，为什么，同时为什么 adcs 这个漏洞能获取域管理员权限，原理是什么
24、内网域渗透中，最新出的 CVE-2022-26923 ADCS 权限提升漏洞需要什么利用条件，原理是什么，相比原来的 ESC8 漏洞有什么利用优势？
25、内网渗透中，如果拿到了一套 vcenter 的权限，如何去进一步深入利用？db 文件如何解密？原理是什么？
26、vcenter 机器拿到管理员密码了，也登录进去了，但是存在一个问题，就是内部有些机器锁屏了，需要输入密码，这个时候怎么去利用？
27、内网权限维持的时候，360 开启了晶核模式，怎么去尝试权限维持？计划任务被拦截了怎么办？
28、mssql 除了 xpcmdshell，还有什么执行系统命令的方式？需要什么权限才可以执行？
29、如果 net group "Domain Admins" /domain 这条命令，查询域内管理员，没法查到，那么可能出现了什么问题？怎么解决
30、查询域内管理员的这条命令的本质究竟是去哪里查，为什么输入了之后就可以查到？
31、免杀中，如何去过国内的杀软，杀软究竟在杀什么？那么国外的杀软比如卡巴斯基为什么同样的方法过不了呢？
32、免杀中，分离免杀和单体免杀有啥区别，为什么要分离，本质是什么？
33、打点常用什么漏洞，请简述
34、内网横向中，是直接进去拿一台机器的权限直接开扫，还是有别的方法？
35、钓鱼用什么来钓？文案思路？如何判断目标单位的机器是哪种协议出网？是只做一套来钓鱼还是做几套来钓鱼？如何提高钓鱼成功率？
36、钓鱼上线的主机，如何进行利用？背景是只发现了一个域用户，但是也抓不到密码，但是有域。

shein（希音）企业蓝军（30k+）

shein 是两次 hr+一次技术面，一面的面试官很有意思，他看了我的 github，有了以下对话
“我看了你的 github，上面有个大厂面经，我要问的问题上面基本都问完了啊，我们就简单过一下好了”
然后他问了一些比较新的问题，主要是涉及云方向的，oss，s3，存储桶，bucket 之类的，确实问的问题没有什么重复的，哈哈哈，还是比较好玩，二面就还是传统的红队面试套路，相关技术栈都问了一遍。

1、oss，s3 存储桶的一些操作，如何利用云主机漏洞进行操作
2、如何利用供应链 类似与 npm 投毒 原理是公司具有私有库和共有库 一般优先查找是通过公有的库来进行查找 然后再是私有的库 然而有的东西 私有库有 公有仓库其实并没有因此可以在共有库上传，可以控制一片主机
3、spring actuator 泄露 heapdump 包括 s3 oss 存储密码 aksk 从而控制桶
4、利用 host 头碰撞碰撞出真实的 host 头，然后直接访问真实的 ip 地址，进而绕过 waf，因为首先是 waf，然后再是 cdn，最后再是真实 ip，直接把 host 头解析到目标位置，可以绕过 waf 直连
5、mysql 的深入利用
6、k8s 的鉴权部分
7、邮件网关 spf 的绕过
8、weblogic fastjson 的原理以及绕 waf 的原理

三快在线（美团）（30k+）
1、java 反序列化原理
2、机器不出网，如何代理进去打内网

深信服（深蓝攻防实验室）
1、内网怎么打 思路
2、国护刷分策略 通用性的寻找通用靶标思路 怎么刷
3、数据库 主机 云 vcenter 刷满是多少分（看你打的多不多 对分的规则熟悉不）
4、内网的多级代理用什么东西代理
5、如果 tcp 和 udp 不出网 用什么策略来进行代理的搭建
6、多级代理如何做一个 cdn 进行中转 具体怎么实现
7、内网有 acl 策略 如果是白名单 如何绕过这个白名单进行出网上线 ip 和域名的都有可能

b 站(30k+)
1、k8s 和 docker 如何去做攻击 有哪些利用方式 是什么原因导致的
2、cs 的域前置和云函数如何去配置
3、内网攻击的时候 内网有那些设备可以利用 （hadoop kibana 之类的设备）
4、攻击 redis 不同的 linux 系统有什么不同
5、sql 注入的时候，如果遇到了返回的时候长度不够，怎么解决，如何截取，用什么函数截取
6、域前置
7、免杀

顺丰(25k+)

1、order by 后面的 sql 注入如何去做利用
2、java 反序列化漏洞原理

中通(25k+)
1、内网有哪些集群化的设备可以打 除了 nas 之类的还有啥
2、内网需要特别注意哪些端口，一个 4 开头的，一个 1 开头的，分别对应哪些服务，有什么利用方式

shopee 红队（Singapore）(30k+)
1、linux 除了基本的内核提权还有什么别的方式可以进行提权
2、如何删除 linux 机器的入侵痕迹
3、寻找真实 ip 的快速有效的办法
4、print nightmare 漏洞利用&分析
5、java invoke 反射具体利用
6、域内常用命令
7、根据子网掩码探测指定资产
8、什么是无状态扫描
9、kerberos 原理
10、ntlm relay 原理
11、内网现在微软至今都没有修复一个漏洞，可以从普通的域用户提权到域管用户，用了 ntlm relay，你讲一下是什么漏洞
12、100 家单位，现在需要在一天时间内拿到所有单位的 ip，port，banner，怎么做，用什么东西来做
13、黄金票据原理，黄金票据在 kerberos 的哪个阶段？如何制作？用哪个用户的 hash 来制作？
14、cs 域前置的原理？流量是怎么通信的？从我直接执行一个命令，例如 whoami，然后到机器上，中间的流量是怎么走的？
15、java 反序列化原理

shopee&seamoney 蓝军(30k+)
1、如何反溯源

长亭:
1、spring spel 漏洞原理&利用方法 什么情况才能利用
2、java jdbc 反序列化高版本不出网的条件下如何利用
3、tomcat becl 如何利用
4、shiro 反序列化用的是哪种加密方法 如何利用
5、ueditor 哪种语言环境存在漏洞 怎么利用 如何绕 waf
6、内网 Windows Print Spooler 利用&原理
7、内网 PotitPetam 利用&原理
8、域内 pth 和工作组 pth 的差别
9、域内用户和工作组用户的差别
10、如何攻击域控
11、spirng4shell&log4j 利用

12、外网常用打点漏洞有哪些
13、一个任意文件读取/任意文件下载，如何进一步利用
14、用友 nc beanshell 执行命令如何过 waf
15、shiro 反序列化漏洞如果 cookie 中的 payload 过长被 waf 拦截如何绕 waf

天融信：
1、内网网闸有什么用，如何去做利用？

---2023 面试题部分---
2023 年了，笔者苟在甲方，已经不在外面乱面试了，但是这个系列一旦有素材还是会更新，素材均来自于笔者朋友面试后新鲜出炉的真题。
JD 企业蓝军（by 饼人）
1.信息搜集
答:我当时是魔改的 shuize 的脚本,通过 hunter,fofa,quaike 的 api 查询相关域名,备案,加到队列,(这部分是调的 lijiejie 的脚本),subdomain 之类的,去重,加到任务队列,绕 CDN,泛解析加到队列,打一些自己添加的 poc
2.java 反序列化的原理,java 怎么执行 shellcode
答:???
3.内存马类型,研究过么
就记得 filler 类型和 serverlet 类型,别的记不得了
4.shiro 不出网的利用,怎么回显,
(这里面试官说了,key 正确和不正确回显内容一致的情况,答了一种用 dnslog 验证 key 正确性的方式,后来问如果不出网怎么办)
答了 shiro 的加密方式,key 是 aes 的 key,两种方式构建回显 tomcat,spring
5.绕 rcf?(没听清,估计是类似终端防护的设备),怎么运行黑 exe
白名单文件:forfile mshta ,powershell,(cmd 肯定不行),这里说了一下 powershell 是调一个 lib 的,通过写个 c#的程序加载这个 lib,也可以执行命令,net 内存加载,defender 的 dll 劫持,(因为之前弄过 nissrv.exe 和 mpclient.dll 的 dll 劫持,现在估计是不行了),还有个释放的方式,exe 释放个 pe 文件再加载,这部分没尝试过,只是看到过样本,他问这种释放的 loader 该怎么写,确实没写过,
6.cs 马的免杀:
dll 劫持,分离免杀分成远程加载和本地加载,内存解密,powershell,还有种没试过的,说是利用 windows 剪切板执行 shellcode
7.域,内网问如何打域控?
答了 zerologon 和 42287,
8.如果域控没有洞呢?
答通过 什么 logon.exe 和 adfind.exe 还有个 powershell 脚本可以查询域用户登陆的主机,找出对应关系和域管登陆的主机,打这些主机,拿到域管 hash,打域控
NTML 中继,之前看到过利用 xss 和 ssrf 中继 NTML hash 的案例
9.adfind.exe 通过什么方式查询的了解过么?
(其他忘了)

---2024 面试题部分---

2024 年了，笔者又不甘寂寞的出来面试了，两个目的，一个是很多人说现在行情不好，想看看是怎么回事；
另一个目的就是和同行交流下，看看大家是怎么做事情的，通过面试学习下别人的经验；
关于行情这块，我觉得从需求理解，其实很多甲方还是需要红队的，属于保障业务的刚需。乙方原先因为业务扩张的原因多招了大量的人，现在市场回冷，这一部分人就都需要裁掉。并且乙方的安全支撑维度，具有一定的局限性，现在更多有钱的甲方喜欢自己招人，自己管理，变成了一个大趋势，因此进一步侵占了原本乙方的一些市场，乙方市场空间再次收窄；所以单纯从市场角度，个人觉得从行业选择思路上切，工作一段时间的中高级网安从业者，甲方肯定是更好的；而初级到中级之间，乙方较好，因为可以接触更多的项目，了解更多的漏洞环境。

网安是一个依托于业务主体的附属行业，附属行业具有被动性，要吃主线业务盈利能力的，如果大规模甲方公司的业务能力都不行了，那么波及到整个乙方甚至网安市场，大家脸色肯定不好看。
因此目前的打算，可能是花两到三个月的时间，面一面目前主流的甲方大厂，实战采样下各家安全团队的相关情况。
至于最后能拿多少钱，不是最终目的，反正市场最后会定价的，更多的其实还是利用外部环境帮助自己反思不足的一个过程。
以下是更新面经

滴滴：
一面：
面试官用了一个腾讯会议的动态壁纸，后面是一只跳动的黄猫，猫猫的头一直在跳动，有时候回答问题的时候会有点出戏；
而且不知道怎么搞的，HR 给我好像投到运营那边去了，因为岗位 JD 上写了什么关于 0Day 分析，Hvv 相关的，一开始还以为也是甲方的红队，最后问他问题的时候，才发现面我的应该是运营的 Leader，他们这边叫反入侵团队。
下面选择一些没有怎么遇到过的面试题记录下来

1. 如果给你一个靶标，靶标的名字就是 xxxx 路灯管理系统，也没有给单位名字，请问怎么去打这个靶标
//当时我说我也没遇到过，确实没遇到过，以往拿到的靶标信息都是有单位名和对应的靶标的名称的，单独给一个模糊靶标的情况很少见，然后面试官看我有点懵逼，分享了一下他的经历
“首先当时我们拿到了一个靶标，名字就叫做 xxxx 路灯管控系统，然后首先归类，这个 xxxx 路灯管理系统，一定是政府下面的，归政府管的，现在范围就缩小到了政府，然后由于互联网上没有直接找到这个 xxxx 路灯管理系统，因此从网络分离情况来看，既然互联网没有，那么这个东西要么在对应单位的私网下，要么在政务网的专网下，后来在专网里面发现了这个系统，然后打下来了。这个系统本身的名字，其实不叫所谓的 xxxx 路灯管理系统，他是在攻防演练之前，改了名字，后来跟裁判证明的时候，F12 找到了对应的前端注释，之前是确实叫这个名字的，只是后来由于攻防的关系，在演练期间改了名字。”
2. shiro 注入内存马的时候，cookie 的过长问题怎么解决
// 这个问题其实我在以前的面试题里面有解决过，还写是因为面试官颗粒度问得很细腻，估计是想筛选掉蒙混过关的人

以下是这个问题的子项拆分
2.1 你是用什么方式实现的 shiro 的后渗透利用，是注入什么马进去
2.2 你实现这个 loader 在 cookie 里面，post 包体里面传的是什么值，是直接传过去，还是说用键值对的形式传过去，为什么
2.3 关于你传入的 post 包体，里面是直接传字节码，还是说传入其他的东西，为什么这么做
2.4 loader 到底是 loader 什么，为什么 loader 加载了就可以完成内存马注入
3. JNDI 注入相关
//这里颗粒度他也拆分得很细腻，以下是子问题
3.1 关于 JNDI 注入，可以利用的协议有哪些
3.2 除了 RMI 还有 LDAP，还有什么其他的协议可以利用吗
3.3 利用 RMI 和 LDAP，分别有什么区别，他们的局限性在哪里
3.4 RMI 和 LDAP 协议的本质是什么，有研究过吗
3.5 JDK 高版本绕过问题，有什么办法绕过 trustbasecode 吗
3.6 除了工厂类，还有什么可以绕过
3.7 工厂类的具体实现怎么操作还记得吗，怎么利用
3.8 降低难度，工厂类一般和哪个中间件配合还记得吗
3.9 除了利用 Tomcat 的工厂类进行绕过，还有什么中间件（提示：Sprintboot）
4. 内存马相关
4.1 说下当今内存马的分类和利用
4.2 关于你说的 Agent 马，具体是怎么操作的
4.3 关于 Agent 马不落地的一些操作
5. 工具相关
问了一下我做的一个攻击面管理和资产巡航工具，用 golang 写的，问了下我实现的思路。
6. 问了下我看没看过设备，HIDS，全流量之类的
//那肯定看过啊，哈哈哈哈，安全职业生涯的必修课，我是从安服仔干起的，咋可能不会看设备

二面+三面+HR 面：
这部分感觉没什么营养，技术相关的问题问得少，大部分都是问一些管理的问题，职业生涯规划的问题，人情世故相关的问题，毕竟是甲方，都是这样的。
他们这个用的是交叉面试，一面二面是安全团队的直属工作人员来面试，三面感觉是个协同部门的 Leader 来面试的，也就是工作交集相关的工作人员。
HR 面的时候，跟我说：“同学，明天我会加一下你的微信，这段时间有问题可以问我”
然后就没有然后了，微信在第二天也没加，这也过了一段时间了，一直也没加。
我估计是当晚面试完，就和业务部门同步情况去了，然后业务那边考虑觉得明显超预算了，就算了。
因为当时她问我期望薪资，我是说的不知道多少，我看市场定价就行。
然后她追问，那么目前你能去的公司，给你开多少。
我给了个挖我的最低价，然后她知道了，大概就能凭经验算一个值出来。
以下再列举下细化的分析
1. 职能冲突问题
HR 面的时候，一定要问我职业规划的问题，我回答滴滴需要什么，我就做什么，反正技术和管理都可以做，就比较圆滑，然后她继续追问，那么不考虑滴滴这边的情况，你自己想做什么，那我回答，那就先技术后管理吧，然后她在最后的时候说了，目前我面的这个岗位是

不需要带人的。
这个很可能就有冲突，因为我目前是带团队的，有管理背景，进去新公司之后会面临双管理困局，那么一山不容二虎的局面又来了，就很伤。
这个问题我想了一下以后被问到了应该怎么回答，我就说我只想做技术，但是目前有管理经验，因为公司给我安排了管理职能。
这个也是实话，但是换一种方式说，就会比较好听，只做技术，工具人属性拉满，然后被安排了管理职能，又表明有管理能力，在面对岗位不确定是否需要带人的时候，属于一个比较中性的回答。
2. 价格问题
现在甲方面试都是先问了你当前的薪资，然后他再去评估，估计这段时间评估去了，可能岗位超预算了；
排除这些笔者主动投递简历去面试的，目前挖笔者的公司给的定级基本在 P7 左右，最多 P7+，肯定没到 P8，但是不是每一个公司都要招 P7 的人，有可能岗位预算只做到了 P6 左右，因此预算和职级不符，就会导致 Drop 的问题。
3. 再看看有没有合适的人
不排除很久以后会再联系，但是情况比较少见，除非真的找不到，那么就要去申请特批预算来招我，但是感觉可能性较小。

附带个题外话，为什么挖我暂时不走，有以下几点原因。

1. 因为笔者核算了实际成本，其实到手的钱差不了多少的。
在打工到中后期，会迎来一个实际到手工资的边际递减效应，主要是由于税率上升和加班增加导致的。
打工的成本，对个人来讲，主要构成为
（实际工作时间）+（通勤成本）+（税）+（房租）+（团队卷度）
上面的东西，核算打工成本的部分可能不完善，但是我觉得覆盖了大头。
拿月薪 80k 举例，年税后到手是 68w。
月薪 50k，年税后到手是 43.7w，中间相差 24.3w。
80k 对应的年薪，不算年终，是 96w。
50k 对应的是 60w。
60w 到 96w 的区间，虽然只有 36w，但是跨到了 p7 这个级别。
工资梯度上去了，税也高了，加班也多了。
那么假如说拿到 96w 的年薪，说一点班不加，这个估计也是天方夜谈。
但是笔者目前还真不加班，早上九点上班，大部分时候晚上六点半就下班了，除开有重大项目的时候。
然后笔者的公司又在郊区，租房成本很低，四五千，可以租一个大套房，这在上海已经很舒服了，而且笔者购置了摩托，天天钻车缝，通勤很快不堵车，因此时间成本和交通也很低。
最关键的一点在于，笔者的工作项目和自己的研究项目是高度重合的，都是主流的软硬件，防火墙，堡垒机，Vcenter，Java 这些，所以上班并不觉得消耗。
而且笔者属于已经成型的红队，自己是知道研究方向和提升路线的，不需要一家公司来教我。
说白了还是，师傅领进门，修行在个人。
老师的作用的确很关键，关键在于，能告诉一条比较快，效率比较高的路线，带一下，然后这样不至于踩很多坑，主要是帮助建立框架。
那么框架成型的基础上，基本都是靠自己研究了，遇到实在搞不懂的，再去找别人请教，这

个也属于单点细节问题解决，不属于框架性的问题。

综上，在各方面成本较低的情况下，笔者利用高度复合的时间，边工作，边追着热点安全问题研究，在不损害身体的情况下（不超额长期加班），每天进步一点，日益变强，其实就维持了一个正向循环。

2. 余量问题

很多人喜欢超出所谓的舒适区域太多做事情，把自己拉到满载来运转，觉得提升很快，这个我承认，确实快，但是一定是需要把身体的折损考虑进去的，因为身体的医疗和健康成本也是成本。

走得快是一方面，走得稳，走得远，更是一方面，毕竟人生是长跑来的。

自己装过主机的应该有经验，假如一个电源，有 2000w 的供电能力，然后去推 1500w 的功耗主机，其实推的还是游刃有余的，还有 500w 的余量，这样电源机器不用一直满负载来工作，发热量不那么大，寿命可以大大延长。

那么假如就恰好使用 1500w 的电源来推呢，电源天天都是满负载工作，要是能不能推动，确实能推动，但是每天都是满载工作，他的发热量那么大，损耗那么高，究竟工作寿命能推多久，有没有 2000w 的电源工作寿命长，这个答案是显而易见的。

转换到工作中，也是一样，要给自己留有余量，很多人可能都没有 1500w 的供电，可能只有 1000，1200，但是强行在推 1500w 功耗的工作，这个是很危险的。

笔者认为，实际的工作能力，并不一定要完全对等于当前工作岗位，可以留出一截余量高于当前岗位，俗称控分。

这样既保证做事能很快做完的同时，另一部分余量可以留作自我发展的空间，因为人是会进步的嘛。

等到余量进一步增加，那么就可以再换到更加具有挑战性的工作岗位上，这样保证年年有余，身体也健康，钱也赚到了，人也一直在进步。

慢就是快，说得不是真的要走得慢，而是稳步提升，真的是最快的路径。

一下搞猛了，容易受伤，然后歇逼又歇逼大半年，然后觉得落下了，又搞猛了，然后又容易受伤，就变成死循环了。