所面试的公司：北京\*\*信安

薪资待遇：保密。不过给到满意了，因为是一线城市，也不会牵涉二三线转一线不加薪的忧虑。而且hr和主管都蛮好的，嘿嘿。

所在城市：北京

面试职位：安全服务工程师

面试过程：电话面试。总共经历了三次面试。还有两三次人力资源的沟通。

面试官的问题：

1. 自我介绍  
   巴拉巴拉~
2. 红蓝队经验  
   巴拉巴拉~ 红队的话主要就是地市级别的多一些，以抢时间为主，一般都是三个人，一般按照1（沟通整理资产）1（打点）1（提交）或者3（整理资产打点利用~）统一提交。还有就是打内网比较赖的话就端口转发，扫弱口令、ms17-010、心脏滴血这些~  
   省级的话基本都在二线，不过也拿过几个靶标~但是内网自己做的很少~  
   其他的问题关于，一些自己的名次相关的就不细说了。  
   蓝队的话还是地市级别的~哈哈哈~主要是配合自己厂商的产品+绿盟的isop之类的平台+其他友商的产品进行溯源分析到ip，封就ok了，没那么多讲究。
3. 关于shiro漏洞了解多少~  
   ps:自己了解吧。java的东西我目前没兴趣。
4. 说说你APP测试的经验~  
   服务端就正常测啊~一般情况下，xposed+fiddler就ok了，不过有些APP不允许模拟器，那就用drony相当于又开了个vpn，app走这个，然后实现抓包，不过得用低版本的安卓机，高版本的有点问题，解决不了。
5. xposed用的什么框架~有没有自己写过app解密~  
   justtrustme~没有~
6. Xss~SSRF~SQL 产生的原因~修复方案~  
   没啥好说的
7. 如果你Xss打了后台，发现是内网的怎么办~  
   emmm，以前确实遇到过，放弃了,hhhhh。让我临场想一想，能不能配合脚本扫下内网啥的，反正我也不会~面试官说没关系~下一问。
8. 假设给你一个目标站，你要怎么做？  
   信息搜集（省略~）授权到位~直接xray配合awvs被动扫（只要不登录就ok）或者直接awvs批量跑，反正效率第一嘛。要求高的话，继续手工给他做精细活呗。 主站功能点多的话，找找功能点呗，没准一个头像上传getshell,蚁剑bypass disable function舒舒服服，之后万一烂土豆啥的提个权，收工。要是真有这么简单，我怕不是直接去红队了，hhhh。这里，大家手法不同，就举个栗子吧~
9. linux和windows提权知多少。  
   linux的什么find提权啊~一大堆~还有烂土豆等等，就注意最高位0755就对了，然后就是最近的sudo提权。windows就内核提权呗，systeminfo,完事。
10. 会不会进程注入？  
    不会。
11. 做过几次应急？  
    没几次，本身应急就少，分到个人身上，也就一两次。一次教育的~没啥意思。一次linux的挖矿~也挺无聊的。
12. 讲讲windows和linux应急你咋做的  
    windows的日志分析那几个pid啥的~linux cronb那几个东西~允许上D盾啥的，直接上去扫一波后门，顺藤摸瓜~分析分析日志等等~这玩意就不细讲了，因为我现在直接做也做不下来，得照着笔记和文档做了。
13. 用过没用过我们家的goby和fofa?  
    goby那肯定用过啊，hvv神器，fofa我还买了个会员呢~  
    ~我们公司入职就送会员~  
    啊~这，有点亏了~~~
14. 会不会apk反编译？  
    加壳的不会，反正客户端的就apktools那些，照着手册做呗，然后就是adb那些。
15. 你python水平咋样？  
    普通的http的脚本还是勉强ok的。问了一些模块re、bs4、request这些~
16. 你php怎么审的  
    目前框架类的还是灰盒为主~巴拉巴拉~你要说pop链，我能多多少少看懂，但是tp的pop链我写不出来，不过普通的ctf里的pop链我还是能写出来的。  
    其他的问题就比较私人了~就不说了。  
    大概就这些吧，其他的问题就是别的公司的安全研究和红队方向的了，也想不起来多少了。  
    别的公司的就简单说一丢丢吧：  
    红队的话，很多主要是思路还有内网的一些，还有就是名次比重。  
    什么shiro不出网，找不到出网机器怎么办~ 上传的马访问不到怎么办~ win2012能不能直接mimikatz获取明文之类的~端口转发~找可用目录~改注册表、注销重启~就不多说了。  
    安全研究的~  
    就tp的sql讲讲~tp的pop链讲讲~自己审的洞讲讲~ 我那么菜我~我~我~讲个窝窝头啊~我曲项向天歌行不行~  
    好了好了，就这了就这了~弟弟太菜了，希望，大佬们能找到自己心仪的工作，然后努力攒钱买房养娃~把安全发展成副业~不是兴趣谁靠安全挣钱啊~hhhhhh~也期待能和大佬未来做同事~hhhh

面试结果：已拿到offer。

面试难度：安服还是蛮简单的。

面试感受：佳。