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。

其实面试每一年都在改变，每一年面的东西，或多或少都会和当年出来的新技术有关系。
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）

//红队&&企业蓝军方向
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

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？