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？