**某服的一个面试小哥，下面是面试问题：**  
1、**上来先问了你知道有什么哪些协议类型**  
当时有点懵，就是只说了HTTP和https协议 TCP\IP协议，其他的协议当时没想起来 后来巩固了下 ARP 地址解析协议 SNMP 网络管理协议 DHCP 动态主机配置协议 FTP 文件传输协议等等  
2、**然后就又问了解不了解OSI七层模型**  
这个还比较在行，大学主修的网络工程对这个模型比较熟悉，当时把七层模型（应用层、表示层、会话层、传输层、网络层、数据链路层、物理层）都说了出来，也说了自己的大学专业。嘿嘿~~  
3、**接着就又问了网络层有哪些协议**  
这个回答的就比较尴尬了，当时只知道各层名称，具体的还真没想起来，就又回答了HTTP 和HTTPS TCP/IP 不过后来查了下回答错了，这个HTTP和HTTPS应该是属于应用层的，但是面试官貌似没在意（估计他也记错了），只给我说了TCP/IP属于传输层····· 其实网络层应该是IP ICMP RIP IGMP这几个协议类型的  
3、**然后他说我是不是很熟悉http协议，那你说一下http协议的一些请求头**  
这个问题也比较不清楚，但是想着也不能说不会，就说了下能具体一点吗  
4、**结果他就说user-Agent是什么 Referer是什么 哪个显示的是IP地址**  
当时一想这不就是BURP抓包里面的数据包嘛，然后就都回答了 使用者代理信息 返回信息 显示IP地址的就是Host了  
5、**然后他又询问你知道哪些常见的端口吗？**  
这个也列举了一些常见的端口开放 21-FTP 22-SSH 27017-Mongo 3306-Mysql 443-https 8080-tomcat  
6、**答完之后又开始拷问我你知道6379是哪个端口吗？**  
当时比较懵 但是也不能说不知道就问是哪种类型的是数据库还是其他中间件啥的  
然后他就直接说了redis，接着又开始问我了解哪些中间件，这个还好都记得  
当时回答了 nginx iis Apache  
7、**接着又问这些中间件的解析漏洞你了解吗？**  
由于这几天都在准备H--W的面试资料，这个印象也比较深刻，先说了IIS6.0的asp目录下默认会解析成asp文件 ISS7.0的.jpg/.php形式的解析 再有就是apache的从右往左的解析规则漏洞 还有就是Nginx的.jpg/1.php 当时回答的比较模糊 但是他好像都没在意 就说还有一个可知名的解析漏洞，想了半天还好回答上了，是00%截断  
8、**接着又问我对CSRF这个漏洞有什么修复建议吗？**  
干脆了断的回答了风哥上课讲的 加token值 当然不能只回答这一个 还要加上自己对这个的理解还有讲一下这个原理，其实主要就是要和面试官多聊一些  
9、**接着就开始问我除了解析漏洞还了解哪些漏洞**  
当时就把正式课程 教的SQL注入 XSS注入 反序列化 文件包含 命令注入的原理以及类型全说了一遍中间还说了几个关键的函数以及一些自己也做了一些漏洞复现 例如：THINKPHP THINKCMF WEBLOGIC的这些远程命令执行漏洞利用，当然还问了修复建议，简单回答就是过滤 + 正则表达式+ 开发人员代码要写的严谨些。  
这些问完之后，才开始询问H--W的问题了  
10、**好像首先问的是你有没有H--W的经验和应急响应的经验**  
这个的话如实回答 没有参加过H--W 但是最近有了解过H--W并知道一些事件等级以及工作分组，应急响应的话这里有做过，就是回答了一些 看看主机有没有异常登录信息(net user) 异常端口开放(netstat -ano) 异常进程(tasklist) 查看一下linux里的/var/log日志 windwos的日志 然后根据攻击者的思路去进行一个信息检查 用D盾检查一下有没有webshell文件。大致就是回答了这些  
11、**然后就又让我举个给客户做应急响应的例子**  
其实还真没咋接触过这一块，但是最近网上看的这些比较多 就随便轻描淡写的描述了一下，具体也忘了。。。总之就是围绕上面回答的措施来描述的，比较片面 后面我又解释说，现在是实习生应急响应这一块的话让我接触的比较少，所以就。。。  
12、**了解一些安全设备吗 防火墙啥的**  
这个的话感觉比较凑巧 昨天刚白嫖了奇安信的HW培训资料（这里吐槽一下 他们那里是先培训基础的知识相当于我们正式课的基础篇 然后笔试——在之后线上学习HW的培训——最后面试后大概是300/天，着实很低） 然后把奇安信的天眼（威胁感知系统）介绍了一些大致的功能-日志分析 注入特征 上传检测(这里评论留言可以免费发给你们~~)然后就又说了一些自己公司的安全设备告警（反弹shell 暴力破解 弱口令）之类的。  
13、**然后就又开始深入询问：假如你现在是研判组的话 对于安全设备的告警事件你如何去判断是否为误报的方法和思路**  
手动验证一下，然后就是根据告警上面的信息去查询，去检验一下  
14、**知道数据流量分析吗**  
这里也很迷不知道怎么回答 就是简单说了自己用过wireshark 用一些过滤规则去分析数据报文 数据包的内容。  
15、**当你来到现场时首先的一个思路加固方案**  
根据一些漏洞扫描工具(nessus awvs appscan)扫描出来的漏洞及时反应给他们去修复，然后就是根据等保制度去修改一些中间件的配置 和系统的配置文件  
16、**假如让你写一份写报告说一下思路**  
这个的话其实也不是很清楚总之脑海里当时就知道 （时间 地点 人物）然后就是围绕这三个回答了 时间 攻击源地址 根据事件类型 漏洞类型去划分，最后再根据自己的经验去总结一下写到报告上。

**面试难度**：难度适中，  
**面试感受**：和面试小哥聊了20分钟，也不知道自己能不能过，过了又能给自己多少薪资 ，感觉自己还是hw这方面的回答不是太好 ，后期还需要加固一下，多看看HW的资料，公众号以及咱们的社区经验。  
**给大家的建议**：多看公众号，多记一下面试官常问的问题比如：H--W中的溯源和应急响应以及安全设备。