一面  
投的是安全服务岗位，但是后面打电话告诉我的是咨询服务顾问，所以当时有点懵逼，完全不知道这个岗位是做什么的。好在面试官电话打来之后大概讲解了下岗位的基本情况，但是更多的是感觉侧重于数据安全，应急响应，我自己也不是很了解，所以感觉有点凉凉。后来找到岗位的要求，

1. 做个自我介绍  
   简单的说了下自己的基本情况
2. xml注入和xxe的区别（一直以为这两个东西是一样的，不过后来百度下发现还是有区别的）  
   xml注入后面百度到的，大家可以参考下
3. 什么是xxe和它的利用方式  
   xxe就是xml解析器令关键词system可以解析外部实体并且没有做任何过滤，导致可以读取本地文件，利用方法可以说下靶场的做法
4. 打过ctf比赛吗，做出来过比赛题吗，讲一下  
   根据自己的经历可以说一下，如果打比赛获得证书的话更是加分项
5. 应急响应怎么做  
   准备相关的工具，查后门等工具  
   初步判断事件类型,事件等级。  
   抑制范围，隔离使爱害面不继续扩大  
   查找原因，封堵攻击源。  
   业务恢复正常水平.  
   总结，报告，并修复、监控  
   以上是常规的回答，想知道你是否有这方面应急相关的经验，像这类问题甲方面试比较多。  
   剩下的时间都是在听面试官讲，不过打电话结束后告诉我当天晚上会有下一次面试，这个效率还是蛮快的！  
   二面（技术面）
6. 做个自我介绍
7. 如何绕过cdn查找真实ip  
   查找二级域名  
   让服务器主动给你发包（邮件）  
   敏感信息泄露  
   查询历史解析ip
8. 文件上传的基本方法，重点是%00截断以及它的原理  
   基本方法可以参考文件上传靶场的做法  
   因为在C语言中字符串的结束标识符%00是结束符号，而PHP就是C写的，所以继承了C的特性，所以判断为%00是结束符号不会继续往后执行  
   条件：PHP<5.3.29，且GPC关闭
9. 解析漏洞有哪些  
   IIS 6.0  
   /xx.asp/xx.jpg “xx.asp”是文件夹名  
   IIS 7.0/7.5  
   默认Fast-CGI开启，直接在url中图片地址后面输入/1.php，会把正常图片当成php解析  
   Nginx  
   版本小于等于0.8.37，利用方法和IIS 7.0/7.5一样，Fast-CGI关闭情况下也可利用。  
   空字节代码 xxx.jpg%00.php  
   Apache  
   上传的文件命名为：test.php.x1.x2.x3，Apache是从右往左判断后缀
10. 讲一下你有意思的渗透测试经历  
    讲了下内网渗透
11. 什么是黄金票据  
    黄金票据是伪造票据授予票据（TGT），也被称为认证票据。如下图所示，与域控制器没有AS-REQ或AS-REP（步骤1和2）通信。由于黄金票据是伪造的TGT，它作为TGS-REQ的一部分被发送到域控制器以获得服务票据。  
    黄金票据的条件要求：  
    域名称[AD PowerShell模块：（Get-ADDomain）.DNSRoot]  
    域的SID 值[AD PowerShell模块：（Get-ADDomain）.DomainSID.Value]  
    域的KRBTGT账户NTLM密码哈希  
    伪造用户名
12. 用过cs吗，如何将msf的会话发送到cs中  
    好像是一条命令具体没记清
13. 知道时间盲注吗，时间盲注用到的函数有哪些  
    ascii substr sleep if  
    三面（压力面）  
    感觉应该是压力面，因为会抓住一个问题问的比较深入  
    我在假期在启明星辰实习过，所以将实习经历在简历上写了一下，后来发现这次实习经历给了我很大的帮助。因为三次面试中都问到了这次实习
14. 你在实习期间都做什么？都用到了哪些设备？回答：入侵检测。你是怎么发现有攻击的？如何判断攻击是误报的？
15. 面试的岗位是咨询服务顾问，但是问到了给你渗透测试岗位你会不会去做？回答：可以试试。但是发现这个给我挖的一个大坑吧。然后问你知道两者的区别吗？说实话对两个工作的概念是很模糊的。
16. 问到还有其他的经历吗。回答:挖过src。都有哪些平台？什么漏洞?你是如何挖掘漏洞的？  
    简单说了下自己挖掘的方法