所面试的公司：\*步  
平台：腾讯会议（语音）  
面试过程：整体流程就是自我介绍加上一些问题问题balabalabala。。。由于面的是蓝队所以渗透部分不会太多，回答部分基本上是我的原答案，不保证正确。面试总体大概分三个大块（下面跳过自我介绍部分）

**面试官的问题：**

**一.操作系统**

* **问：linux命令熟悉吗？**
* 答：了解过一些。（其实不熟）
* **问：查看进程的命令有哪些？**
* 答：top、ps
* **问：还有吗？**
* 答：不记得了。（pstree应该也是一个）
* **问：查看网络进程的命令？**
* 答：netstat
* **问：linux如何加密md5？**
* 答：不会
* **问：那问个简单点的，如何快速查看文件类型？**
* 答：ls、ll  
  还有一两个问题没记住，反正我不会。。。

**二.渗透测试**

渗透测试部分问的比较基础，也不多

* **问：说下sql注入？**
* 答：回答上课教的内容就可以了。
* **问：讲下xss？**
* 答: 还是上课内容。我是说了xss三种类型，分别有哪些特点。三种触发方式。
* **问：反射型xss和dom型xss的区别？**
* 答：我的回答是“dom型xss是通过修改或读取docunment的属性和方法进行攻击，既有反射型也有存储型，而且没有与服务器进行交互。”
* **问：看你挖过src讲讲你挖过觉得比较有趣的漏洞？**
* 答：按照实际情况答即可。

**三.应急响应**

* **问：linux被上传了webshell如何查杀？**
* 答：首先top查看进程，是否有cpu占用率特别高的以及ID是随机数的，可以尝试kill进程，再次查看还会不会出现（这里感觉不太好）。然后可以用ps -ef|gred查看进程详细信息，用/proc找到进程，cp+sz下载文件放入\*步在线云沙箱进行分析。确认是木马就删除文件。再cat /etc/rc 排查开机启动项和cat /etc/crontab 排查定时任务，last，lastlog等排查日志和可疑用户。  
  **- 问：除了杀进程还有什么方法可以快速找到webshell吗？因为有时候占用率高的不一定是木马，也可能是业务相关进程**
* 答：不了解。
* **问：日志会看吗？**
* 答：有看过，主要是时间，源ip和请求内容等等，还有登录日志。windows还有事件码balabla。（这里网络不好不知道什么时候掉线了）
* **问：刚才你讲到哪了？**
* 答：不好意思我不知道什么时候掉线的。
* **问：那这个问题跳过，你了解护--网是做什么的吗？**
* 答：护--网行动是一个攻防演练活动。我们蓝队是防守放，应该主要分为两组，一组对流量和报警进行监控，一组进行应急响应和溯源。先期会对企业的资产进行梳理和预渗透来进行一个加固。
* **问：最后一个问题，在一个很大流量的环境中，如何快速对报警进行一个判断？**
* 答：如果是大量相同源ip发起的请求，首先判断是不是一个误报。如果是内部问题导致的误报可以请求甲方进行整改，如果甲方拒绝整改就把这个拉入白名单。同样如果是大量相同的源ip对同一个ip或者网段有大量报警，可以考虑是扫描器或者爆破，比如查看参数，己方是java搭建的网站，却出现了php的语句，可以判断是扫描器在扫描。（最后面试官告诉我有四种情况，但是我忘了。。）  
  面试结果： 通过

面试难度：一般

面试感受：蓝队还是要多了解应急响应和安全设备

给大家的建议：面试蓝队linux和windows的命令一定要多了解一些，应急响应和溯源都是必须了解的内容