1. 参加过什么项目（hw、渗透）
2. 往年护网担任的职位
3. 用过哪些安全设备（设备细节）
4. 参与过红队（看看是否了解攻击手法）
5. 蓝队防守应该着重哪些点去防守（判断防守思路，是否参与过应急和前期规划）
6. 怎么判断真实红队攻击和网络蠕虫扫描（判断基础流量分析能力，如果不清楚。可定为初级）
7. 如果护网监测发现资产有被攻击情况，应该怎么去解决（判断一下是否有良好思路，会不会通过分析流量去查看是否攻击成功，如果有思路可往中级以上推）
8. 如果内网机器发起了扫描，应该怎么去解决（判断是否有应急响应能力，如果这块不错可往高级上推）
9. 如果客户要求去溯源，溯源的思路有哪些，怎么去溯源（判断溯源能力，高级的加分项）
10. Windows和linux排查命令和思路（判断是否有上机排查能力）