常用面试题整理By珍惜Q&V:296488320

逆向方面：

1. hook框架使用： xposed 和frida. 各有什么优势以及实现原理。
    - frida原理：
    - xposed原理：
2. IDA的使用，常用的快捷键，常见的使用技巧。
3. so调试经验：如何过so的加固，混淆以及反调试。
4. elf文件格式：
5. IO重定向原理和做的事情以及如何检测IO的重定向。

   检测CRC.检测mmap
6. unidbg是否使用过，so是如何还原。以及如何检测

   只支持23 26 的sdk
7. 如何检测rpc

   hook invoke 的调用栈
8. 加壳和脱壳了解吗？都做过哪些加壳的方式。
9. 抓包软件用过哪些：tcp的包如何获取和分析的。

android framework 层知识：

1. so的加载过程
2. app的启动过程
3. 如何动态代理Android service
4. VA的实现原理

语言方面知识：

ARM汇编

1. thumb指令和arm指令的区别
2. r0~r15 寄存器的作用

C和java

1. extern 关键字。
2. static 关键字。
3. C++多态的实现原理
4. 宏定义中的# 和 ## 的区别

JS相关

1. web逆向的常用方式
2. 浏览器环境和指纹相关：环境补齐做了哪些？指纹补齐做了哪些？
3. js混淆和还原：如何应对js fuck的混淆。
4. 是否了解AST，如何还原。

5. chrome. Dev 常用的功能
6. 油猴插件是否用过，做了哪些事情?
7. 小程序的解包，抓包过程。
8. chrome 抓包，如何处理websocket的包

加密算法的知识：

1. AES 、DES 、MD5 的算法特征
    - DES
    - AES 常用的对称加密算法，有ECB和CBC 模式。算法将数据按照16字节分割，不足的补齐。
        - ECB模式：分别对不同的数据段做分别加密，然后合称为一块。
        - CBC模式：是一种循环模式，前一个分组的密文和当前分组的明文异或操作后再加密，这样做的目的是增强破解难度。
        - Padding作用：AES是固定长度块加密，当明文大小不是整数倍块长度的时候，就需要在明文后边加上填充，同时需要填充能够还原成明文是很好的去除。
    - MD5：
    - BASE64：

扩展能力

1. 是否发表过什么帖子。
2. 资源如何获取的，如 微信号资源，微信协议资源，账号资源。
3. 通过什么渠道了解新的技术。