2023年了，笔者苟在甲方，已经不在外面乱面试了，但是这个系列一旦有素材还是会更新，素材均来自于笔者朋友面试后新鲜出炉的真题。

JD企业蓝军（by 饼人）

1.信息搜集
答:我当时是魔改的shuize的脚本,通过hunter,fofa,quaike 的api 查询相关域名,备案,加到队列,(这部分是调的lijiejie的脚本),subdomain之类的,去重,加到任务队列,绕CDN,泛解析加到队列,打一些自己添加的poc
2.java反序列化的原理,java怎么执行shellcode
答:???
3.内存马类型,研究过么
就记得filler类型和serverlet类型,别的记不得了
4.shiro不出网的利用,怎么回显,
(这里面试官说了,key正确和不正确回显内容一致的情况,答了一种用dnslog验证key正确性的方式,后来问如果不出网怎么办)
答了shiro的加密方式,key是aes的key,两种方式构建回显tomcat,spring
5.绕rcf?(没听清,估计是类似终端防护的设备),怎么运行黑exe
白名单文件:forfile mshta ,powershell,(cmd肯定不行),这里说了一下 powershell是调一个lib的,通过写个c#的程序加载这个lib,也可以执行命令,net内存加载,defender的dll劫持,(因为之前弄过nissrv.exe和mpclient.dll的dll劫持,现在估计是不行了),还有个释放的方式,exe释放个pe文件再加载,这部分没尝试过,只是看到过样本,他问这种释放的loader该怎么写,确实没写过,
6.cs马的免杀:
dll劫持,分离免杀分成远程加载和本地加载,内存解密,powershell,还有种没试过的,说是利用windows剪切板执行shellcode
7.域,内网问如何打域控?
答了zerologon和42287,
8.如果域控没有洞呢?
答通过 什么logon.exe和adfind.exe还有个powershell脚本可以查询域用户登陆的主机,找出对应关系和域管登陆的主机,打这些主机,拿到域管hash,打域控
NTML中继,之前看到过利用xss和ssrf中继NTML hash的案例
9.adfind.exe 通过什么方式查询的了解过么?
(其他忘了)