**问：打点一般会用什么漏洞**

优先以java反序列化这些漏洞像shiro，fastjson，weblogic，用友oa等等进行打点，随后再找其他脆弱性易打进去的点。因为javaweb程序运行都是以高权限有限运行，部分可能会降权。

**问：平常怎么去发现shiro漏洞的**

登陆失败时候会返回rememberMe=deleteMe字段或者使用shiroScan被动扫描去发现

完整：

* 未登陆的情况下，请求包的cookie中没有rememberMe字段，返回包set-Cookie里也没有deleteMe字段
* 登陆失败的话，不管勾选RememberMe字段没有，返回包都会有rememberMe=deleteMe字段
* 不勾选RememberMe字段，登陆成功的话，返回包set-Cookie会有rememberMe=deleteMe字段。但是之后的所有请求中Cookie都不会有rememberMe字段
* 勾选RememberMe字段，登陆成功的话，返回包set-Cookie会有rememberMe=deleteMe字段，还会有rememberMe字段，之后的所有请求中Cookie都会有rememberMe字段

**问：shiro有几种漏洞类型**

shiro 550

shiro 721

**问：weblogic权限绕过有没有了解**

<https://blog.csdn.net/weixin_45728976/article/details/109512848>

好像是用./进行绕过的

**问：fastjson漏洞利用原理**

具体：<https://www.cnblogs.com/hac425/p/9800288.html>

回答：在请求包里面中发送恶意的json格式payload，漏洞在处理json对象的时候，没有对@type字段进行过滤，从而导致攻击者可以传入恶意的TemplatesImpl类，而这个类有一个字段就是\_bytecodes，有部分函数会根据这个\_bytecodes生成java实例，这就达到fastjson通过字段传入一个类，再通过这个类被生成时执行构造函数。

**问：weblogic有几种漏洞**

weblogic就好多了，基于T3协议的反序列化；基于xml解析时候造成的反序列化，还有ssrf，权限绕过等等

**问：IIOP听说过吗，和什么类似**

java RMI通信，也就是远程方法调用，默认是使用jrmp协议，也可以选择IIOP。

**问：这几个漏洞不出网情况下怎么办**

让这几个漏洞回显

**问：拿到webshell不出网情况下怎么办**

reg上传去正向连接。探测出网协议，如dns，icmp

**问：dns出网协议怎么利用**

将域名解析指向自己的vps，然后设置ns记录等等，不记得了

**问：横向渗透命令执行手段**

psexec，wmic，smbexec，winrm，net use共享+计划任务+type命令

**问：psexec和wmic或者其他的区别**

psexec会记录大量日志，wmic不会记录下日志。wmic更为隐蔽

**问：Dcom怎么操作？**

通过powershell执行一些命令，命令语句比较复杂，不记得了

**问：抓取密码的话会怎么抓**

procdump+mimikatz 转储然后用mimikatz离线读取

Sam 获取然后离线读取

**问：什么版本之后抓不到密码**

windows server 2012之后（具体我也忘记了）

**问：抓不到的话怎么办**

翻阅文件查找运维等等是否记录密码。或者hash传递、或者获取浏览器的账号密码等等。

**问：域内攻击方法有了解过吗**

MS14-068、Roasting攻击离线爆破密码、委派攻击，非约束性委派、基于资源的约束委派、ntlm relay

**问：桌面有管理员会话，想要做会话劫持怎么做**

提权到system权限，然后去通过工具，就能够劫持任何处于已登录用户的会话，而无需获得该用户的登录凭证。终端服务会话可以是连接状态也可以是未连接状态（这里当时没答上来，觉得有点鸡肋。我也不知道是不是这个意思）

面试难度：中-  
面试感受：由于面试习惯了，面试不带紧张。面试的攻击手法其实也就这些，懂了就ok