

2020/2/18 深信服深圳一面

面试前一天hr电话预约时间下午五点，面试时间还是很准确的-大概也是半个小时（不知道为啥问了一些系统漏洞，哭了）

一、介绍

实习时间，能否去深圳

二、实战经验

描述其中分数最高的一个洞

三、struct2漏洞原因

四、反序列化漏洞

分别回答php,java,python

五、windows-rdp漏洞-是系统漏洞吧，真就不熟了

他应该想问0708吧

<https://www.cnblogs.com/backlion/p/11482322.html>

六、免杀，病毒

webshell混淆吧

七、计算机基础

八、python熟悉么

九、linux和windows不同点导致的漏洞

晕了-讲了一个文件解析漏洞问题

十、你想实习学到什么

十一、ATT&CK框架中的横向攻击

<https://www.anquanke.com/post/id/187998>

能否复现里面的攻击模式

内网服务器有ssh,有多少总方式进入

socket5跳板，ssrf,frp?不知道是不是这个意思，他说att&ck模型上写了四五十总。orz

十二、聊了一下他们的业务