二面

自我介绍

sql

子域名挖掘

设备，全流量设备

告警有上传，怎么判断有没有上传成功

告警webshell已经确定上传了有多个马你怎么定位排查

告警cs已经确定上传并且处置了你怎么定位排查干净了

你上传了cs你怎么做权限维持

自我介绍

2，设备应急场景题

3，http协议常见字段

4，waf绕过经验

5，红队思路

6，去年蓝队成果

7，挖src的思路

8，安全设备

自我介绍

渗透思路

应急经历

信息收集思路

sql注入一般怎么测，用什么工具

内网渗透有没有做过

log4j有没有进行过勘测

逻辑漏洞遇到过哪些，未授权漏洞遇到过哪些

有没有参加过国护

设备用过哪些

自我介绍（介绍项目）

渗透测试思路及用到的工具（根据你提到的接下来发散提问）

windows下有哪几个可以自启动的目录

水平越权，垂直越权的思路，改哪些参数导致（自己提到的）

修改注册表哪里可以导致自启动（维权的操作）

shiro,log4j2

windows，linux怎么应急

个人pc被钓鱼，删了webshell但是还会有cs流量怎么办

设备用过哪些

事件id，创建用户id

1.提权

2.sql注入利用

3.反序列化

4.安全产品

5.木马等病毒的处理，以及定时任务(从红队蓝队的方面考虑)

6.溯源

7.告警的误报处理

9.最近拿到什么样子的漏洞

10.IP过流量的溯源

11.日志排查

12.hw期间都做过负责哪些

13.做过哪些等保

工作经历，hw期间的事件，渗透测试的整个流程，信息收集的具体过程，应急做过的具体情况