1. **你有没有毕业？**

已经毕业，正在工作（实习）

1. **护网预计在6月份（7月份），时间问题？**

没有问题

1. **简历有护网经历，你能谈谈护网的情况吗**

根据简历，以及掌握的知识，大胆的说，角色为防守方，工作位监控组，主要使用ips，ids等设备做流量监控与日志分析工作

1. **你能大概说一下，比如数据包或者日志，你的分析思路是什么，以及你会用到哪些工具或者那些网站进行查询？**

用流量监测的安全设备，比如天眼，查看报文，分析报文里和源ip和网站目录路径，查看是否可疑，使用微步在线之类的查询是否为恶意，使用wireshark对数据包深度分析

看一下请求的网站路径，源IP与目的ip地址，host字段的值以及发包内容等

工具有wearshark等，网站的话微步在线等

1. **文件上传和命令执行，有看过相关日志吗**

文件：可能在系统有上传功能或者有文本编辑器，看一下保重是否有base64加密或者url加密，解码验证一下是否有恶意代码

系统日志：有没有web容器做了一些危险行为，比如bash反弹shell等

网络应用日志：有没有异常的网站文件，类似webshell等，就有可能是命令执行

1. **文件上传攻击特征？**

能够上传文件的接口，应用程序对用户上传文件类型不校验或者校验不严格可绕过，导致任意类型文件上传，攻击者可上传webshell。

1. **用过Nmap扫描工具吗**

用过，具体见信安面试，nmap扫描基础命令

1. **常见命令注入漏洞？php? Strust2 ?**

见常见攻击告警分析以及strust2漏洞

1. **你在分析数据包的时候，这个地址是一个互联网的地址，你会做一些什么样的排查或者说对IP地址进行什么样的处理呢？**

把这个域名或者ip放到微步上检测一下，看一下是不是恶意链接

1. **你有用过微步吗？**

这里自己去了解一下微步在线，注册一个账号，试用一下

1. **你做过渗透测试的工作吗**？

有做过，具体看面试50题之2，渗透一个网站需要步骤

1. **你能说明文件上传的原理吗？**

常见的攻击告警，文件上传部分

1. **文件上传加固方法？**

常见的攻击告警，文件上传部分

1. **暴力破解加固方法？**

1.添加强度较高的验证码，不易被破解。

2.修改密码设置规则，提高用户的密码强度。

3.同一账号登陆次数锁定，生成锁定日志。

4.定期排查弱口令。

1. **Sql注入加固措施**？

常见的攻击告警，sql注入部分

1. **你对应急和溯源有过一些了解吗？**

详见：攻防演习应急预案各类安全事件应急处置手册

溯源详见：溯源的思路 文档

1. **一台主机在内网进行横向攻击，你应该怎么做？**

确定攻击来源，是不是员工内部误操作，比如询问运维是否有自动化轮训脚本

如果没有，确定是攻击，结合时间点，根据设备信息，看一下安全事件，进程，流量

找到问题主机，开始应急响应流程：准备，检测，遏制，根除，恢复，跟踪，具体的操 作要交给现场运维去处理。

1. **你能说说护网的流程吗？**

护网流程详见群内课程第二，三课

1. **你还用过其他态势感知的产品吗？**

Ips，ids，hids，堡垒机等

1. **平时windows, linux用的多吗，Linux应用端口，比如常用数据库接口？**

25:SMTP简单邮件传输服务器端口

23:telnet的端口，telnet是一种可以远程登录并管理远程机器的服务

22:ssh端口，PcAnywhere建立TCP和这一端口的连接可能是为了寻找ssh，这一服务有许多弱点

53：dns端口

3306:MySQL的默认端口

1433:SQLServer的默认端口

3389：远程桌面登录

7001:Freak88,Weblogic默认端口，Weblogic是一个application server,确切的说是一个基于JAVAEE架构的中间件

445:是一个毁誉参半的端口他和139端口一起是IPC$入侵的主要通道

139：属于TCP协议，是为NetBIOS Session Service提供的，主要提供Windows文件和打印机共享以及Unix中的Samba服务

1. **命令行工具用的什么比较多？**

Xshell，这个自己下载用一下，连接自己的linux虚拟机就行

1. **应急响应流程**

准备，检测，遏制，根除，恢复，跟踪，报告一般是从第二步到第五步的过程，截图等

准备：信息收集，工具准备

检测：了解资产情况，明确影响，尝试进行攻击路径溯源

遏制：关闭端口，服务，停止进程，拔网线

根除：通过杀毒软件，清除恶意文件，进程

恢复：备份，恢复系统正常

跟踪：复盘全貌，总结汇报

具体操作看 攻防演习应急预案各类安全事件应急处置手册

1. **什么是跨域，JSONP与CORS**

什么是跨域？

跨域：指的是浏览器不能执行其它网站的脚本，它是由浏览器的同源策略造成的，是浏览器的安全限制！

同源策略

同源策略：域名、协议、端口均相同。

浏览器执行JavaScript脚本时，会检查这个脚本属于那个页面，如果不是同源页面，就不会被执行。

JSONP跨域

只支持GET请求，不支持POST等其它请求，也不支持复杂请求，只支持简单请求。

CORS跨域

支持所有的请求，包含GET、POST、OPTOIN、PUT、DELETE等。既支持复杂请求，也支持简单请求。

JSONP与CORS的使用目的相同，并且都需要服务端和客户端同时支持，但CORS的功能更加强大。

JSONP和CORS的优缺点

1. JSONP的主要优势在于对浏览器的支持较好；虽然目前主流浏览器都支持CORS，但IE9及以下不支持CORS。

2. JSONP只能用于获取资源（即只读，类似于GET请求）；CORS支持所有类型的HTTP请求，功能完善。

3. JSONP只会发一次请求；而对于复杂请求，CORS会发两次请求。

应用场景

如果需要兼容IE低版本浏览器，无疑，JSONP。

如果需要对服务端资源进行操作，无疑，CORS。

其他情况的话，根据自己的对需求的分析来决定和使用。

1. **如何检测webshell**

静态检测

静态检测通过匹配特征码，特征值，危险函数函数来查找webshell的方法，只能查找已知的webshell，

动态检测

webshell传到服务器了，黑客总要去执行它吧，webshell执行时刻表现出来的特征，我们称为动态特征。

日志检测

使用Webshell一般不会在系统日志中留下记录，但是会在网站的web日志中留下Webshell页面的访问数据和数据提交记录。

语法检测

语法语义分析形式，是根据php语言扫描编译的实现方式，进行剥离代码、注释，分析变量、函数、字符串、语言结构的分析方式，来实现关键危险函数的捕捉方式。这样可以完美解决漏报的情况。但误报上，仍存在问题。

1. **三次握手与四次挥手**

三次握手（three-way handshaking）

1.背景：TCP位于传输层，作用是提供可靠的字节流服务，为了准确无误地将数据送达目的地，TCP协议采纳三次握手策略。

2.原理：

1）发送端首先发送一个带有SYN（synchronize）标志地数据包给接收方。

2）接收方接收后，回传一个带有SYN/ACK标志的数据包传递确认信息，表示我收到了。

1. 最后，发送方再回传一个带有ACK标志的数据包，代表我知道了，表示’握手‘结束。

四次挥手（Four-Way-Wavehand）

 1）第一次挥手：Client发送一个FIN，用来关闭Client到Server的数据传送，Client进入FIN\_WAIT\_1状态。

 2）第二次挥手：Server收到FIN后，发送一个ACK给Client，确认序号为收到序号+1（与SYN相同，一个FIN占用一个序号），Server进入CLOSE\_WAIT状态。

 3）第三次挥手：Server发送一个FIN，用来关闭Server到Client的数据传送，Server进入LAST\_ACK状态。

 4）第四次挥手：Client收到FIN后，Client进入TIME\_WAIT状态，接着发送一个ACK给Server，确认序号为收到序号+1，Server进入CLOSED状态，完成四次挥手

1. **http状态与无连接**

一.无连接

1. 每一个访问都是无连接，服务器挨个处理访问队列里的访问，处理完一个就关闭连接，这事儿就完了，然后处理下一个新的
2. 无连接的含义是限制每次连接只处理一个请求。服务器处理完客户的请求，并收到客户的应答后，即断开连接

二.无状态

     1.协议对于事务处理没有记忆能力

     2.对同一个url请求没有上下文关系

     3.每次的请求都是独立的，它的执行情况和结果与前面的请求和之后的请求是无直接关系的，它不会受前面的请求应答情况直接影响，也不会直接影响后面的请求应答情况

     4.服务器中没有保存客户端的状态，客户端必须每次带上自己的状态去请求服务器

1. **什么是路由表**

在计算机网络中，路由表（routing table）或称路由择域信息库（RIB, Routing Information Base），是一个存储在路由器或者联网计算机中的电子表格（文件）或类数据库。路由表存储着指向特定网络地址的路径（在有些情况下，还记录有路径的路由度量值）。路由表中含有网络周边的拓扑信息。路由表建立的主要目标是为了实现路由协议和静态路由选择。

每个路由器中都有一个路由表和FIB(Forward Information Base)表：路由表用来决策路由，FIB用来转发分组。路由表中有三类路由：

（1）链路层协议发现的路由（即是直连路由）

（2）静态路由

（3）动态路由协议发现的路由。

1. 非sql数据库

Zookeeper，HBase、Redis、MongoDB、Couchbase、LevelDB

1. Linux 系统安全加固需要注意的内容

1、关闭不必要的系统服务

2、更改SSH默认端口

3、禁止root用户远程ssh登录

4、限制用户使用SU命令切换root

5、密码复杂度策略

6、检查密码重复使用次数限制

7、检查是否存在空口令账号

8、禁止同时按下ctrl+alt+del 重启

9、禁用telnet服务

1. 冰蝎，蚁剑，菜刀的流量特征

[**冰蝎动态二进制加密WebShell特征分析**](https://www.freebuf.com/articles/web/213905.html)

[**常见WebShell客户端的流量特征及检测思路**](https://www.freebuf.com/column/204796.html)

1. 常见OA系统

自己搜一下，记一下就好

1. 横向越权漏洞的修复

横向越权：横向越权指的是攻击者尝试访问与他拥有相同权限的用户的资源  
 纵向越权：纵向越权指的是一个低级别攻击者尝试访问高级别用户的资源

对于纵向越权，我们可以通过设置用户角色，为不同的角色提供不同的权限来避免。

为了防止横向越权，我们可以使用缓存来进行辅助，当登录成功或者进行操作时，我们在缓存中存储一对由用户名和一个唯一的数字组成的数据（token），然后返回放入的唯一数据。在重置密码时我们的参数不仅需要用户名和密码还需要前面生成的唯一数字，根据用户名在缓存中取出对应的数字，如果取出的数字和参数中传入的想等，则证明重置的当前用户的密码，否则不是，且不予以重置。

1. 挖矿病毒

[挖矿病毒，自己搜搜](https://zhuanlan.zhihu.com/p/139019250)

1. 多看看其他提供的材料。