1. 把握主体，回答关键点
2. 细节
    - 例如防火墙如何设置规则、端口、网段
3. 没有很简单的题目，查不到答案
4. 6、8章不考
5. 不考具体的技术，代码实现
6. 可能会考过程
7. 没有名词解释
8. 访问控制、防火墙和IDS注重对比，优缺点

第一章

1. P2DR模型
2. PDRR模型
3. 信息安全管理发展顺序

第二章

1. 攻击的准备、实施、善后阶段做什么；每个阶段的重点内容

第三章

1. 为什么有这么多扫描方法，各自的优缺点
2. 怎么监听，需要什么条件
3. 共享式、交换式怎么监听
4. ARP欺骗过程

第四章

1. dos有哪些方法
2. 攻击的**原理、如何防范**
3. ddos和dos区别，克服了那些弱点，为什么依然没有有效的防御方法、如何防止被追查

第五章

1. 根本原因、危害
2. 不直接写payload，但可能考怎么写，有哪些过程，每个过程要注意什么问题，要注意什么条件，如何覆盖返回地址，如何有防护怎么解决，如何送到目标机，如果不能跳到堆栈应该怎么跳，windows和linux下有什么不同(为什么会有这种不同)
3. 在哪些不好的编程习惯下有可能发生(不安全库、类型不安全)
4. 如何防止缓冲区溢出的发生(软、硬件)

第七章

1. 什么条件下dns/email/web/ip/arp欺骗，如何实施，欺骗的结果(对于攻击者和受骗者)，如何检测和防范

第九章

1. 行：主体能操作什么；列：客体能被谁操作；管理口令；

2. MAC和DAC的区别，典型的实现方式，优缺点
3. RBAC的基本形态，有哪些参与元素，有哪些改进，给一个案例怎么应用RBAC(分配角色、基数约束、运行时约束)
4. 5种身份认证方法、典型实现方式、对谁做身份认证，给出方案(某个场景验证指纹、口令？kerberos不适合超大集群，邮件不能使用challenge-response、什么是对的什么是错的)
5. 隔离方法(隔离网卡、隔离网闸(为什么比防火墙更加安全(不会直接传数据包，内外网不能同时连接，所有基于应用层以下的行为都无效，只可能在应用层进行攻击)))

第十章

1. 不考基本概念
2. 两种典型的实现方式(包过滤，应用层代理)的常见实现，优缺点
3. 规则的匹配规则(优先匹配，第一条匹配，最优匹配)
4. 各种体系结构，代价，优缺点(给场景选择一个具体的体系结构并配置规则(画表)，自己假设网段，给出相应规则的描述)；通常使用画图的方式作答(标注内外网、网段)
5. ftp注意控制端口和数据端口(主动模式和被动模式)

第十一章

1. 状态转换
2. 动态安全访问技术？和防火墙对比
3. 重要的部件，如何工作，优缺点
4. 检测方法的原理，优缺点，给一个场景如何使用(理由)
5. 什么是FP和FN，如何取得平衡，调整系统
6. 日志(追溯)，入侵检测可能是滞后的，通过哪些角度可以获取信息，如何进行分析
7. 基于主机和基于网络(优缺点)
8. 如何响应(阻断攻击、修复损失、挡住未来的同类攻击)
9. 反击、蜜罐(引流，带偏方向，分析攻击者信息加强防御)
10. IPS(加入防御功能)

第十二章

1. 在不安全的网络上建立起安全的信道(防止窃听、防止伪造)
2. 软件+硬件(usb)+pwd
3. 有一个场景，如何设计vpn架构
4. 隧道的模式(IPSec的工作方式)