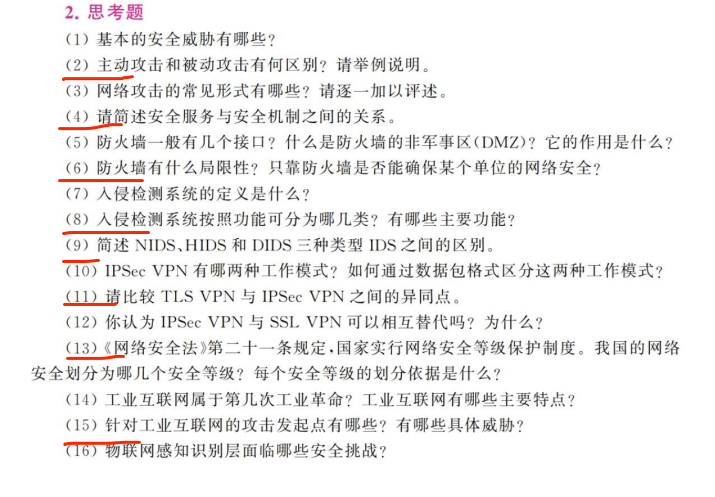
第三章



二、

主动攻击  
特性：恶意篡改数据流或伪造数据流等攻击行为  
分类：伪装攻击、重放攻击、消息篡改、拒绝服务（阻止或禁止人们正常使用网络服务或者管理通信设备）

被动攻击  
特性：对所传输的信息进行窃听和监测  
分类：窃听攻击、流量分析

Tip:被动攻击难以检测但是容易阻止，主动攻击容易检测但是难以阻止

1. 安全服务和安全机制之间的关系：

安全机制是用来实施安全服务的机制，安全机制既可以是具体的、特定的，也可以是通用的，安全服务是指计算机网络提供的安全防护措施。

1. 防火墙的局限性：

1.无法防御内部攻击，

2.对绕过防火墙的连接无用

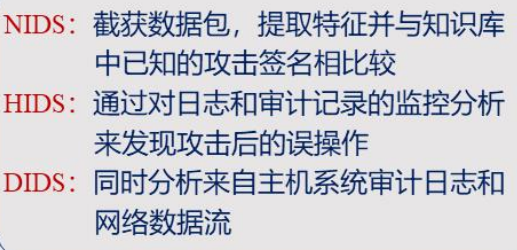
仅靠防火墙无法保证某单位的网络安全

八、入侵检测系统按照功能可分为哪几类

按数据来源---基于网络的、基于主机的、分布式入侵检测系统

按策略---误用检测、异常检测、完整性分析

九、



不同点：数据来源不同，实时性不同，误报率不同，价格不同

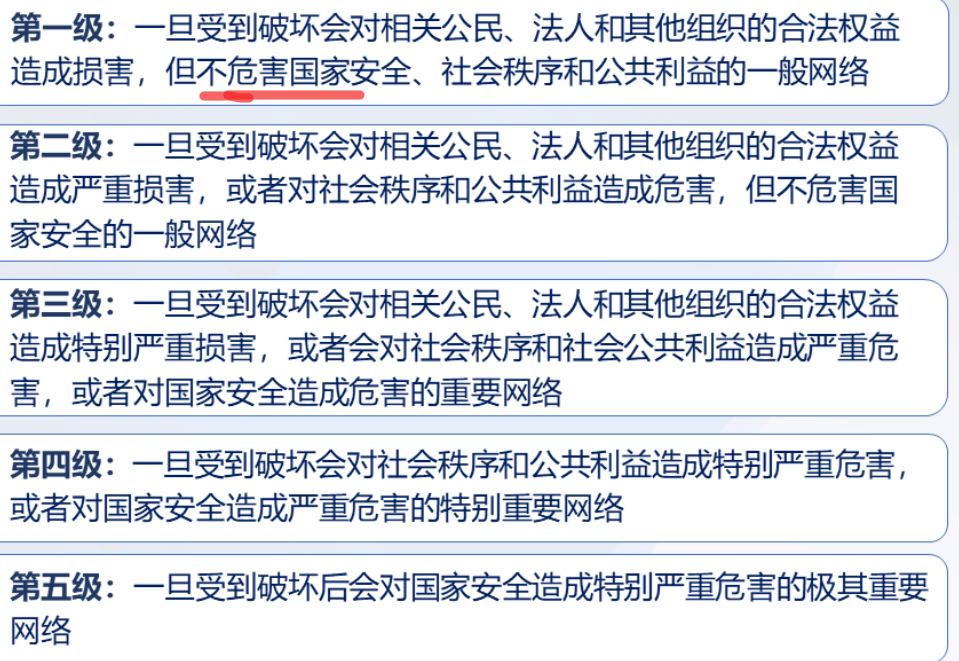
相同点：都是审计跟踪检测数据 监视入侵活动

十一、比较TLS VPN 与IPSes VPN之间的异同点

相同点：身份验证采用双向身份验证和数字证书

不同点:加密方式不同，安全性不同，可访问性不同，费用不同，安装时间不同，使用难易程度不同，用户群体不同，可伸缩性不同，穿越防火墙可行性

十三、网络分为五个安全保护等级。



十五、针对工业互联网的攻击发起点有物理层，网络层和控制层，如：硬件入侵，木马病毒，网络攻击社交攻击等