第一讲 网络安全概述

测试点 1-1

1、 什么是网络安全？

从本质上来讲，网络安全就是网络上的信息安全。网络的安全是指网络系统的硬件、软件及其系统中的数据受到保护，不会因偶然或者恶意的因素的影响而遭到破坏、更改或泄露，系统能够连续、可靠地正常运行，网络服务不被中断。

2、 什么是脆弱性？脆弱性分为哪几类？

所谓网络系统的脆弱性，是指系统的硬件资源、通信资源、软件及信息资源等存在的弱点和缺陷。

i. 硬件系统的脆弱性

ii. 软件系统的脆弱性

iii. 网络和通信协议的脆弱性

iv. 管理的脆弱性

v. 用户的脆弱性

3、 什么是安全威胁？

可能对系统或组织造成危害的不期望事件的潜在原因。脆弱性的普遍存在是安全威胁产生的根本原因。

安全威胁分为哪几类？

信息泄露、完整性破坏、 服务拒绝、 未授权访问

4. 什么是安全攻击？

任何危及到信息安全的行为，安全攻击要利用一个或多个系统的脆弱性。

安全攻击分为哪几类？

被动攻击、 主动攻击、 物理临近攻击、 内部人员攻击、 配装分发攻击

测试点 1-2

1、 什么是安全服务？

安全服务是指提供数据处理和数据传输安全性保护的方法。

什么是安全机制？

安全机制是保护信息与信息系统安全技术措施的总称

常见的安全服务与安全机制有哪些？

安全服务：认证服务、访问控制服务、数据保密服务、数据完整性服务、不可否认服务

安全机制：加密、数字签名、访问控制、数据完整性、鉴别交换、业务流填充、路由控制、公证

2、 安全服务和安全机制的关系是什么？

a) 安全服务体现网络信息系统的安全需求

b) 安全机制是实现安全服务采取的具体技术措施

c) 安全服务与安全机制是多对多的关系

i. 安全服务可以用不同的安全机制来实现

ii. 安全机制可以用来实现不同的安全服务

3、简要说明在应用层、网络层、传输层和链路层部署安全服务的优缺点？

应用层

优点：对数据的实际含义有充分的理解、不必依赖操作系统来提供这些服务、对用户想要保护的数据具有完整的访问权，因而能很方便地提供一些服务、安全策略和措施通常是基于用户制定的

缺点：改动太多，出现错误的概率增大，为系统带来更多的安全漏洞、对现有系统的兼容性太差、效率太低

传输层

优点：现有的和未来的应用可以很方便地得到安全服务、提供了更加细化的基于进程对进程的安全服务、能为其上的各种应用提供安全服务

缺点：由于传输层很难获取关于每个用户的背景数据，实施时通常假定只有一个用户使用系统，所以很难满足针对每个用户的安全需求

网络层

优点：密钥协商的开销小、网络层支持以子网为基础的安全、主要优点是透明性

缺点：无法实现针对用户和用户数据语义上的安全控制

链路层

优点：整个分组（包括分组头信息）都被加密 ， 保密性强

缺点：使用范围有限，只有在专用链路上才能很好地工作 ， 中间不能有转接点