第一次作业

（1）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。

主要有：

a) 硬件系统的脆弱性
b) 软件系统的脆弱性
c) 网络和通信协议的脆弱性
d) 管理的脆弱性
e) 用户的脆弱性

3. **什么是安全威胁？安全威胁分为哪几类？**

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。

威胁的主要类型：

1. 信息泄露
2. 完整性破坏
3. 服务拒绝
4. 未授权访问

4. **什么是安全攻击？安全攻击分为哪几类？**

任何危及到信息安全的行为为安全攻击，安全攻击要利用一个或多个系统的脆弱性。

主要类型：

1. 被动攻击
2. 主动攻击
3. 物理临近攻击内部人员攻击
4. 配装分发攻击

（2）测试点 1-2

1. **什么是安全服务？什么是安全机制？常见的安全服务与安全机制有哪些？**

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，常见分类有认证

服务，访问控制服务，数据保密性服务，数据完整性服务，不可否认性服务。

安全机制是保护信息与信息系统安全技术措施的总称，主要包括加密，数值签名，访问控制，数据完整性，鉴别交换，业务流填充，路由控制和公证。

2. **安全服务和安全机制的关系是什么？**

第一个，安全服务体现网络信息系统的安全需求。

第二点，安全机制是实现安全服务采取的具体技术措施。

第三点，安全服务与安全机制是多对多的关系。其中安全服务可以用不同的安全机制来实现，而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？**

应用层安全服务的优点：

1. 对数据的实际含义有着充分的理解
2. 不必依赖操作系统来提供这些服务
3. 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
4. 安全策略和措施通常是基于用户制定的

应用层安全服务的缺点：

1. 改动太多，出现错误的概率大增，为系统带来更多的安全漏洞
2. 对现有系统的兼容性太差
3. 效率太低

网络层安全服务的优点：

1. 密钥协商的开销小
2. 网络层支持以子网为基础的安全
3. 主要优点是透明性

网络层安全服务的缺点：

1. 无法实现针对用户和用户数据语义上的安全控制

传输层安全服务的优点：

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

传输层安全服务的缺点：

1. 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

链路层安全服务的优点：

1. 整个分组（包括分组头信息）都被加密 ，保密性强

链路层安全服务的缺点：

1. 使用范围有限