1.

（1）简述数字签名的原理 2‘

（2）数字签名技术是如何保证数据的完整性、不可否认性和来源认证的？6‘

（3）数字签名与消息认证技术有什么联系与区别？2‘

2.

现在考虑一个TCP SYN欺骗的情景。假设服务器端的TCP连接表有512个表项，对于每个未建立的连接，每隔30s重新发送一次连接请求，重复7次后将表项删除。

（1）简述TCP SYN欺骗攻击的原理 2‘

（2）假设初始时TCP连接表已被洪泛，为保证TCP连接表始终被填满，攻击者应以什么速率发送数据包？4‘

（3）假设一个TCP数据包为40字节，忽略成帧消耗，求攻击消耗的带宽 4‘

512 / 210 = 每秒发送2.438个数据包

780.19 bps

3.

考虑如下代码：

void hello(char \* tag){

    char data[12];

    gets(data);

    printf("your %s is %s\n",tag,data);

}

（1）假设输入长度为19字节时程序运行不会崩溃，那么输入“Computer Security”后，程序会输出什么？3‘

（2）假设输入长度为19字节时程序不会崩溃，而输入长度为20字节时程序崩溃，如果想要修改tag的话，输入长度应至少为多少字节？为什么？4‘

（3）修改上述代码以避免安全隐患。3‘

4.

（1）三种云服务部署模型分别是什么？3‘

（2）若想在云上搭建自己的操作系统，应该采取哪种部署模型？为什么？3‘

（3）如何加固云上的操作系统？4‘

5.

（1）用户认证方法有哪些？4‘

（2）为防止明文口令泄露和离线字典攻击，应如何储存口令相关信息？4‘

（3）假设一个用户有8个属性，每个属性有10个值，如果采用基于角色的访问控制，应设置多少个角色？4‘

（4）考虑sql语句：

SELECT \* FROM userdata WHERE UID = $\_GET["uname"] AND PASSWORD = $\_GET["password"];

该语句有无安全隐患？攻击者如何在不知道任何用户名和口令的情况下，如何攻击得到全部信息？4‘

（5）为防范（4）中的攻击，应采用何种防火墙？为什么？4‘

附加：State the different levels at which encryption can be applied to a database.

Can be applied to the entire database, at the record level, the attribute level, or level of the individual field