一、填空题

1、信息系统建设的起点和源头是**信息系统安全风险评估**。

2、信息系统安全风险分析涉及**资产、威胁、脆弱性**等三个基本要素。

3、评价资产的三个安全属性是**保密性、完整性、可用性**。

4、威胁的基本属性包括**威胁主体、威胁的对象、动机、出现频率**。

5、信息系统基本安全需求包含**可信和可控**。

6、基本安全技术需求包含**物理安全、网络安全、系统安全、应用安全和数据安全及备份恢复**等5个层面。

7、基本管理要求包括**安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理**等5个方面

二、选择题（包括单选和多选）

1、残余风险是由以下原因造成（**ABC**）

A. 安全措施不当造成的；

B. 安全措施失效造成的；

C．综合考虑了安全成本与效益后未去控制造成的；

D. 组织机构变化后，引入的风险。

2、以下安全措施属于预防性安全措施的有（**AD**）

A. 防火墙；B. 入侵检测；C. 入侵容忍；D. 访问控制

3、以下说法正确的是（**AB**）

A. 根据威胁及威胁利用脆弱性的难易程度判断安全事件发生的可能性；

B. 根据威胁出现的频率和脆弱性的严重程度判断安全事件发生的可能性；

C. 根据资产的价值和脆弱性的严重程度判断安全事件发生的可能性；

D. 根据威胁出现的频率和资产的价值判断安全事件发生的可能性

4、以下说法正确的是（**ABDE**）

A. 脆弱性识别需要具体到每个资产或组件上；

B. 安全措施的确认不需要具体到每个资产或组件上；

C. 保护性安全措施可以降低安全事件发生的可能性；

D. 保护性安全措施可以减少安全事件发生后对组织或系统造成的影响；

E. 安全措施的实施是以减少脆弱性或降低安全事件发生的概率为目标的。

4、以下说法正确的是（**B**）

A. 资产的重要性可以选择保密性、完整性和可用性上的任何一个赋值表示；

B. 资产的重要性只能综合考虑保密性、完整性和可用性上赋值；

C. 资产的重要性取决于资产的经济价值；

D. 资产的重要性取决于资产的价值。

5、以下哪种情况会出现欠保护（**B**）

A. 在资产价值级别大于威胁级别的情况下，以威胁级别作为信息系统（安全域）的安全保护等级；

B. 在资产价值级别小于威胁级别的情况下，以资产价值级别作为信息系统（安全域）的安全保护等级；

C. 在资产价值级别与威胁级别相同的情况下，该级别则为信息系统（安全域）的安全保护等级；

D. 根据信息系统安全等级不同，采用不同的安全措施。

三、简答题

1、信息系统安全风险评估的概念？

**信息系统安全风险评估是依据有关信息系统安全技术与管理标准，对信息系统及尤其产生、处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程。它主要评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响。**

2、在什么情况下进行信息系统安全风险评估？

**设计规划或升级信息系统时；**

**需要增加新的应用或新的扩充时；**

**发生安全事件后；**

**组织发生结构性变动时；**

**按照某些规定或特殊要求，对信息系统的安全进行评估时。**

3、信息系统安全风险评估的可控性原则是什么？

**服务可控性；**

**人员与信息可控性；**

**过程可控性；**

**工具可控性。**

4、什么情况下会造成残余风险？

**残余风险是指采取安全措施后信息系统仍然可能存在的风险，即未被安全措施控制的风险。**

**残余风险有些是由于安全措施不当或无效造成的，而有些则是在综合考虑了安全成本与效益后未去控制的风险。**

5、风险评估工具选择的原则？

**实际需要原则：**

**首先必须清楚风险评估工具的运行平台和应用平台；**

**在选购时，一定要注意工具是否能够检测最新操作系统所特有的安全问题；**

**工具除了对TCP/IP协议进行分析外，还应该能够分析其他网络协议。**

**试用原则：**

**购买前，测试或试用一下，在用户的实际环境和系统下看看工具能否有效。**

**实用原则。**

**风险评估工具不仅能够找出特定系统的安全弱点，帮助管理员修补漏洞，而且能够提供风险分析报告；**

**应具有良好的人机界面，能够通过互联网为用户提供有关漏洞的详细说明、风险程度、修补措施等。**

**满足脚本数量与更新速度要求：**

**评估工具脚本的数量并不一定与漏洞的数量成正比；**

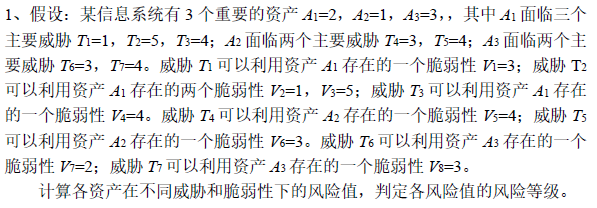
**必须留意工具的更新频率，看它是自动更新的，还是手工更新，以及发现威胁后，它需要多长时间才能推出新版本。**

**支持不同级别的入侵检测：**

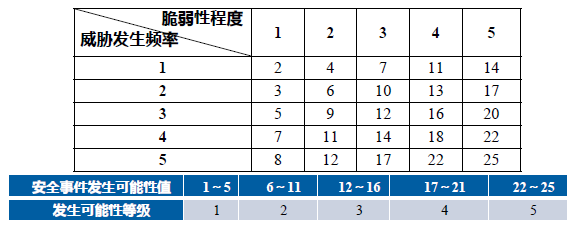
**在高访问量期间，对担负关键任务的系统不应运行风险评估工具；**

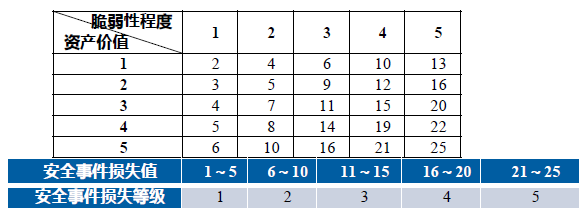
**初步选定风险评估工具后，必须进行必要的试用，看看它的实际使用效果和效率怎样**

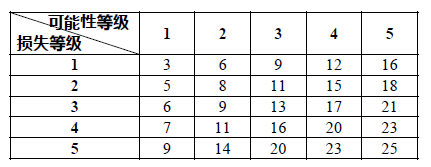
四．计算题

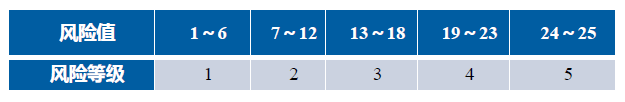


**使用矩阵法，根据课件中的三个矩阵以及值和等级的关系表：**

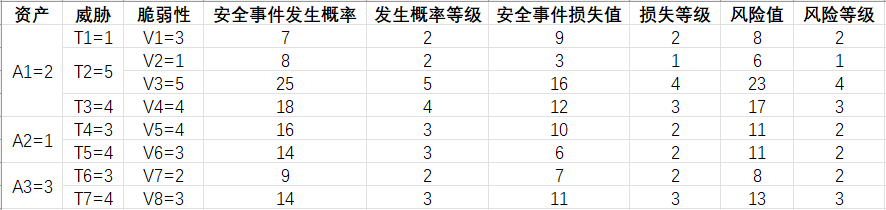








**计算得到下表：**



**最后一列为计算出的风险等级。**