**2017年信息安全工程师考试下午试题加答案（六）**

新开的**信息安全工程师考试**分属该考试“信息系统”专业，位处中级资格。大家在找试题做练习的时候是否苦恼没有资源？希赛软考学院为大家整理了一些下午试题的练习，供大家参考，希望能有所帮助。

阅读下列说明，回答问题1至问题4，将解答填入答题纸的对应栏内。

【说明】

日志分析就是对有关操作系统、系统应用或用户活动所产生的一系列的计算机安全事件进行记录和分析的过程。在计算机系统中，安全管理员采用日志分析审计系统来监视系统的状态和活动，并对日志文件进行分析、及时发现系统中存在的安全问题。

一个安全的网络系统中的日志分析审计系统，是对网络系统中任一或所有安全相关事件进行记录、分析和再现的处理系统。对于日志分析审计系统的一般要求主要包括：

1、记录与再现：要求审计系统能够记录系统中所有的安全相关事件，同时，如果有必要，应该能够再现产生某一系统状态的主要行为；

2、入侵检测：分析审计系统应能够检查出大多数常见的系统入侵的企图，同时，经过适当的设计，应该能够阻止这些入侵行为；

3、记录入侵行为：分析审计系统应该记录所有的入侵企图，即使某次入侵己经成功，这时候调查取证和系统恢复必不可少的；

4、威慑作用：应该对系统中具有的日志分析审计系统及其性能进行适当宣传，这样可以对企图入侵者起到威慑作用，又可以减少合法用户在无意中违反系统的安全策略；

5、系统本身的安全性：必须保证日志分析审计系统本身的安全性，其中，一方面包括操作系统和软件的安全性，另一方面包括分析审计数据的安全性；一般来说，要保证日志分析审计系统本身的安全，必须与系统中其他安全措施，例如认证、授权、加密措施等相配合。

一个日志分析审计系统的简单模型包括两个部分：日志数据采集器，它用于采集数据；日志数据分析器，它负责对分析审计数据采集器发送给它的日志数据进行分析。

【问题1】（2分）

根据说明，日志分析审计的功能包括（）（可多选）

A、对潜在的攻击者起到震慑或警告

B、对于已经发生的系统破坏行为，提供有效的追纠证据

C、为系统管理员提供有价值的系统使用日志，从而帮助系统管理员及时发现系统入侵行为或潜在的系统漏洞

D、能检测并查杀计算机病毒保证计算机系统的安全

【问题2】（3分）

日志分析方法通常有以下三种，请将该描述的选项对应到其中。

1、基于正则表达式的模式匹配日志分析（）

2、基于关联分析的日志分析（）

3、基于聚类分析的日志分析（）

A、用一定数量的样本（称为训练样本集），由这些样本及其己知类别，给出一套分类判别准则，使得按照这套分类判别准则，对待识别模式进行分类使错误识别率最小。训练完毕后，对任何一个样本，都可以利用分类器将其归到某类中。

B、是数据挖掘中最活跃的研究方法之一。给定一个日志数据库，通过用户指定最小支持度和最小可信度来寻找合适关联规则的过程。

C、可以用于模式匹配和替换的强有力的工具，可以让用户通过一系列的特殊字符构建匹配模式，然后捏匹配模式与数据文件、程序输入以及Web页面的表单输入等目标对象进行比较，根据比较对象中是否包含匹配模式，执行相应的程序。它通常在对日志文件的初步分析中使用。

【问题3】（2分）

一般关联规则挖掘问题可以划分成两个子问题，一是通过用户给定的最小支持度（minsupport），寻找所有频繁项目集（FrequentItemset），即满足support不小于minsupport的项目集。事实上，这些频繁项目集可能具有包含关系。一般地，我们只关心那些不被其他频繁项目集所包含的所谓频繁大项集（FrequentLargeItemset）的集合。这些频繁大项集是形成关联规则基础。二是通过用户给定的最小可信度（minconfidence），在每个最大频繁项目集中，寻找confidence不小于minconfidence的关联规则。根据描述写出这两个子问题名称。

【问题4】（8分）

通过典型的基于关联分析的Apriori算法进行日志分析得出的是特征模式，例如通过对用户历史数据的分析，发现如下关联规则：

模式：username=A,timestamp=am，hostip=192.168.1.119,userip=192.168.1.201[0.98,0.60]

则该模式表示用户A通常在每天的上午登录，登录的主机是192.168.1.119，登录时的IP地址是192.168.1.201，该模式的置信度为98%，支持度为60%。

（1）根据上述方法，请分析模式：username=A,command=vi,param=.c[0.45,0.05]。其中，command表示用户经常执行的命令，param表示执行命令时所使用的参数（3分）

如果在Apriori算法的基础上加上一个时间约束则是时间序列分析算法，它用于分析不同审计记录之间的相关性。它的形式为：X，Y→Z[C,S,w]，X,Y,Z为项集，W为时间约束。含义：若X,Y发生，则在w秒内，Z也发生。

S=Support(XYZ)是规则的支持度：满足规则的样本百分比。

C=Support(XYZ)/Support(XY)是置信度：当X，Y发生时Z发生的条件概率。

系统调用序列与时间序列分析不同的是它只有一个支持度，没有时间窗口的限制，也没有置信度。

如：通过对用户A所执行的命令序列进行分析，发现如下序列模式：

command=vi,param=.c→command=gcc,param=-g-o→command=gdb(0.4)

（2）请分析该模式的含义。（3分）

（3）假设以上的三个模式是挖掘出的关联规则和序列模式，试对其进行分析。（2分）

**参考答案**

一、ABC

二、CBA

三、发现频繁项目集、生成关联规则

四、用户a经常执行的命令为vi，执行命令的参数为.c，置信度为45％，支持度为5％。该用户经常执行命令的序列为：首先用vi编译，通过gcc再编译，最后通过gbd调试。该用户为c程序员，经常上午工作，使用192.168.1.201的客户机登录到192.168.1.199的主机进行工作。