1 分布式入侵检测，即针对分布式网络攻击的检测方法和使用分布式的方法来检测分布式的攻击，其中的关键技术是检测信息的协同处理与入侵的全局信息的提取。1 分

2 智能化入侵检测吗， 及使用智能化的方法和手段进行入侵检测。就是利用智能化的方法进行入侵特征的辨识与泛化。利用专家系统的思想来构建入侵检测系统也是常用方法之一。特别是具有自学习能力的专家系统，实现了知识库的不断更新与扩展，是入侵检测系统的防范能力不断增强，因而具有更广泛的应用前景。2 分

3 全面的安全防御方案，即使用安全工程风险管理的思想与方法来处理网络安全问题，将网络安全作为一个整体工程来处理。从管理、网络结构、加密通道、防火墙、病毒防护、入侵检测多方位对所关注的网络全面加以评估，然后提出可行的解决方案。2 分

叙述题（第 1 题 10 分，第 2 题 8 分，共 18 分）

1 叙述通用入侵检测系统模型的主要部件组成，并绘图表示

答

通用的入侵检测模型主要部件包括事件产生器，活动记录器和规则集三个。如图 1 所示。 2 分

事件产生器是模型中提供系统活动信息的部分。事件来源于系统审计记录、网络通信或者如防护墙、鉴别服务器等应用子系统。 2 分

规则集可视为一个确定入侵是否发生的参考引擎。基于规则的专家系统通常是早期 IDS 的推理工具。Denning 的模型允许采用统计方法把规则集看成是一个核查事件和状态数据的普通检查器引擎，使用规则、模型、模式和统计结果来对入侵行为进行标志。 2 分

活动记录器保存被监视的系统和网络的状态。当事件在数据源中出现时，就改变活动记录器中的变量，活动记录器会根据规则集检查出的活动创建新的变量。 2 分

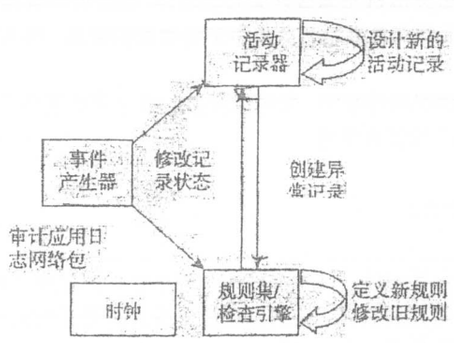

图 1

2 电子证据数据分析包括哪些内容?

答

首先，要进行一系列的关键词搜索以获取最重要的信息。可以利用一些自动取证的文本搜索工具来帮助发现相关信息。 2 分

其次，对文件属性、文件的数字摘要和日志进行分析，根据已经获得的文件或数据的用词、语法和习作（编程）风格，推断出其可能的作者。如果允许利用数据解密技术和密码破译技术，则可以对电子介质中被保护的信息进行强行访问以获取重要信息。 2 分

第三，评估 Windows 交换文件、slack 空间、未分配的磁盘空间因为这些地方都存放者犯罪者容易忽视的证据，可以通过专业的取证公司或相关软件找到犯罪者的犯罪证据。 2 分

第四，对电子证据做一些智能相关性的分析，即发掘同一事件的不同证据间的联系。随着计算机分布式技术的发展，犯罪者往往在同一时间段内对目标系统做分布式攻击以分散管理员的注意力，在分析电子证据时，应对其进行关联分析。 2 分

第五，取证专家完成电子证据的分析应给出证明。

在计算机取证的最后阶段，应整理取证分析的结果供法庭作为诉讼证据。重要的是对涉及计算机犯罪的日期和时间、硬盘的分区情况，操作系统的版本，运行取证攻击时数据和操作系统的完整性、计算机病毒评估情况、文件种类、软件许可证以及取证专家对电子证据的分析结果和评估报告等进行归档处理。 2 分