HW9

PB17111614 王嵘晟

1、审计：记录和分析用户使用信息系统过程中的相关事件。安全审计是对系统安全的审核、稽查与计算。

主要功能：安全审计自动响应、安全审计数据生成、安全审计分析、安全审计浏览、安全审计事件存储、安全审计事件选择等。

2、数字取证作用：打击违法犯罪的作用

(1).发现和归档证据和线索

(2) 固定其他途径发现的证据

(3) 帮助揭示事件模型

(4) 关联攻击和受害的计算机

(5).展现端到端侵害事件的路径，不管侵害是否已遂

(6).提取隐藏、删除或其他不能直接得到的数据

以及：排除故障、日志监控、数据恢复、数据提取、完善策略

3、电子证据特点：

①数字性：物质载体是电子元器件和磁性材料等。

②技术性：产生、储存和传输及其采集、分析、判断都必须借助计算机技术、存储技术、网络通信技术。

③脆弱性：电子证据脆弱、不可靠。

④.多态性：表现形式多

⑤人机交互性：形成时不同环节上有不同人员参与，施加不同影响。

⑥复合性

4、数字取证步骤：

①.收集：发现潜在的数据源，获取数据

②检查：通过评估数据与特定事件的关联性，从收集的数据中提取信息、

③分析：分析提取的数据进而依据系统的方法得出结论

④报告：依据分析写出报告

5、证据信息类别：

①来自软件的数据

②来自操作系统的数据

③来自网络的数据

④来自应用软件的数据