第九次作业

PB19111708 杨云皓

UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA
Hefei,Anhui.230026 The People's Republic of China

1. 对国内外发生的有关计算机安全的事件进行实时响应与分析，提出解决方案和应急对策，保证计算机信息系统和网络免遭破坏

2. 所谓审计，简单地说就是记录和分析用户使用信息系统过程中的相关事件，安全审计主要功能为为事后处理提供重要依据，为网络犯罪行为和泄密行为提供取证基础

3. 通过调查可疑的计算机和网络系统，收集和保存证据，重建事件，评估事件的状态，获得证据从而进行犯罪调查或响应一个计算机安全紧急事件，获得证据，打击违法犯罪

4. 还可：排除故障，日志监控，数据恢复，数据提取，完善策略

4. 数字性，
技术性
脆弱性：数据的修改可以在瞬间完成
多态性：电子证据的表现形式可是多种多样的
人机交互性：不同计算机操作人员的参与并会对电子证据施加不同影响
复合性：电子证据是多种形式证据的集合

5. 收集：发现潜在的数据源并从中获取数据
检查：评估数据与特定事件的关联性，从收集的数据中提取信息
分析：分析提取的数据进而依据系统的方法得出结论
报告