网络犯罪全景透视

——计算机犯罪取证手册

作者　[美]德博拉·利特尔约翰·欣德
埃德·蒂特尔（技术编辑）
译者　高卓

目　录

- 保护网络装置

密码学基本概念

- 加密安全的目的
  - 认证身份
  - 提供数据保密性
  - 确保数据完整性
- 基本加密概念
  - 通过代码和密码混杂文本
  - 什么是加密？
  - 通过密码算法确保数据安全
  - 信息安全中的加密应用
  - 什么是隐蔽术？
  - 现代破解密码的方法
  - 网络罪犯对加密和隐蔽术的利用

基于硬件和软件的安全方案

- 实施基于硬件的安全措施
  - 基于硬件的防火墙
  - 认证装置
- 实施基于软件的安全措施
  - 加密软件
  - 数字证书
  - 公钥基础设施
  - 基于软件的防火墙

防火墙

- 防火墙分层过滤
  - 数据包过滤
  - 电路过滤
  - 应用过滤
- 一体化入侵检测

组建事件响应小组

制定和实施安全政策

- 安全以政策为根基
  - 什么是安全政策？
  - 这个问题为什么对调查人员关系重大？
- 评估安全需要
  - 机构安全计划的组成部分
  - 定义各方面责任
  - 分析风险因素
  - 评估威胁和威胁级别
  - 分析机构和网络的脆弱性
  - 分析机构因素
  - 考虑法律因素
  - 分析成本因素
  - 评估安全解决方案