

安全审计、攻击和威胁分析

课程目录

第一课：安全审计绪论

- 安全审计的概念
- 风险评估
- 风险评估的执行过程
- 漏洞分析
- 确定资源的优先级
- 从不同角度考虑编制审计计划
- 获取管理者的建议
- 审计人员的职责和前瞻性
- 获取客户的回馈

第二课：审计过程

- 检查书面的安全策略
- 识别正常的商业活动
- 使用现有的管理控制体系
- 使用主机级和网络级的扫描软件发现主机的漏洞
- 考虑路由器和防火墙配置
- 确定电话系统的安全级别
- 评估现有备份行为的有效性

第三课：发现资源阶段的审计

- 发现方法
- 安全扫描
- 物理侦测
- 刺探
- 应用企业级的审计工具
- 你能获得什么信息？

第四课：渗透和攻击阶段的审计

- 网络渗透技术
- 攻击的指纹
- 常见服务的安全
- 确定攻击目标
- 路由器
- 数据库
- WEB 服务器和 FTP 服务器
- E-mail 服务器
- Naming 服务
- 审计系统 bug
- 审计陷阱和 rootkits

- 审计拒绝服务攻击
- 综合性的攻击策略
- 非法服务

第五课：控制阶段的审计

- 控制阶段的审计内容
- 控制方法
- 渗透到其他系统
- 实施控制阶段的审计
-

第六课：审计和日志分析

- 日志分析
- 建立基线
- 防火墙和路由器日志
- 操作系统日志
- 日志过滤
- 审计可疑的活动
- 其他类型日志
- 日志存储
- 审计和运行效率的关系

第七课：审计结果

- 创建评估报告
- 考虑报告的阅读者
- 制作详尽的报告
- 推荐审计方案
- 提高可行性
- 审计和安全标准
- 提高路由器安全
- 开启预警功能
- 主机审计解决方案
- 升级和替代服务