安全审计、攻击和威胁分析

课程目录

- 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