操作系统安全

课程目录

第一课：安全原则
- 网络安全的一般原则
- 面临的公共安全威胁
- 商业级的操作系统所应具备的功能
- 保护账户
- 灵活的访问控制
- 网络安全的三角模型
- 安全策略
- 检验系统状态

第二课：Windows 安全基础
- Windows 中的身份认证
- 基于域的安全
- 访问控制
- NTFS 权限
- 操作系统的常规漏洞
- Windows 系统的常规漏洞
- 注册表的概念及作用
- 服务器消息块协议
- MIME 和 APIs

第三课：高级 Windows 安全

- 文件系统安全
- Windows 的默认设置
- Windows 的日志
- 注册表安全
- 服务包和补丁包

第四课：UNIX 和 Linux 安全
- 操作系统的常规漏洞
- 缓冲区溢出、配置错误和 root kits
- UNIX 的认证机制
- UNIX 的访问控制
- 密码过期和账户停用

第五课：UNIX 和 Linux 安全基础

- UNIX 权限
- 可拔插的认证模块 PAM
- 使用 Tripwire 实现基于主机的入侵检测
- 易受攻击的服务
- NFS 简介
- Telnet 的安全
- Apache 的安全
- 数据库安全
- SSH 简介及运用
- FTP 安全
- UNIX 日志管理

第六课：特殊的操作系统安全

- 思科 IOS 操作系统
- 交换机和网桥安全
- 管理网络设备
- 无线访问点的安全
- 附加设备安全
- 硬件升级
- 升级测试
- 建立计划更新

第七课：降低风险

- 简化功能降低风险
- 补丁包和修复程序
- 禁止和删除不必要的服务
- 持续的进行监控

第八课：计算机取证

- 计算机取证定义
- 专用处理技术
- 收集和标识信息
- 保存好相关的有用信息
- 取证技术
- 驱动器分析
- 文件恢复
- 代码分析
- 内存和文件系统搜索
- 取证软件
- 创建报告