网络安全基础与防火墙

第一课：安全的概念

- 网络安全的背景
- 建立有效的安全矩阵来保护资源
- 网络安全和企业投资回报率
- 识别风险和威胁
- 存在 100%的安全吗

第二课：安全标准和安全组织

- 网络安全的国际标准
- ISO 1779
- ISO 27001
- 网络安全的国家标准
- 网络安全组织
- CERT
- SANS
- OCSE

第三课： 网络安全的要素

- 网络安全的概念和安全机制
- 网络安全的元素
- 安全策略
- 安全元素----加密
- 安全元素----认证
- 特殊认证技术
- 安全元素----访问控制
- 安全元素----审计
- 寻求网络安全的平衡点

第四课：应用加密

- 加密的好处
- 创建信任关系
- 理解加密术语：轮、并行加密和加密强度
- 对称密钥加密
- 对称加密算法举例
- 非对称密钥加密
- Hash 加密
- 加密的执行过程

- 使用 PGP 和 GPG 对邮件和文件进行加密
- 公共密钥体系结构 PKI
- 在企业中运用 PKI
- PKI 术语和技术
- 数字签名
- 一次性密钥加密(OTP)

第五课：攻击基础

- 网络攻击行为的动机
- 暴力破解和字典攻击
- 系统 bug 和后门攻击
- 拒绝服务和分布式拒绝服务攻击
- ping 扩散攻击
- SYN 洪水攻击
- 死亡之 ping 和 LAND 攻击
- 缓冲区溢出攻击
- 社会工程学和非直接攻击
- 网络钓鱼欺骗攻击
- 信息泄密攻击
- 间谍软件和广告病毒攻击

第六课：高级攻击

- 欺骗和中间人攻击
- 嗅探攻击
- 链路劫持和 TCP 握手攻击
- 病毒攻击
- 特洛伊木马
- 非法服务攻击
- 键盘记录
- SQL 注入
- Web 涂鸦攻击
- 基于浏览器的攻击（帧欺骗）
- 对攻击进行响应和阻断

第七课：一般安全原则

- 通用安全原则
- 通用安全原则----偏执狂
- 通用安全原则----建立有效的网络安全策略
- 通用安全原则----不要采取单独的系统和技术
- 通用安全原则----将损害降低到最小程度
- 通用安全原则----在企业中部署强制执行策略
- 通用安全原则----提供培训
- 通用安全原则----根据需求购置设备

- 通用安全原则----正确识别正常的商业行为和活动
- 通用安全原则----考虑物理安全

第八课：防火墙和虚拟局域网

- 防火墙的功能
- 防火墙术语
- 防火墙的默认配置
- 创建包过滤防火墙的规则
- 包过滤的优缺点
- 配置代理服务器
- 远程访问和虚拟局域网
- 防火墙对常见服务（Web，E-mail，VoIP，FTP）的保护
- 合理的选购防火墙设备
- 防火墙日志
- 防火墙的周边环境
-

第九课：防火墙设计

- 通用防火墙设计原则
- 非军事化安全区 DMZ
- 创建屏蔽子网防火墙
- 创建筛选路由器
- 创建单宿主防火墙
- 创建双宿主和多宿主防火墙
- 防火墙硬件安全问题
- 运用多种技术的组合来设计防火墙体系

第十课：设计安全的网络

- 考虑拓扑结构的安全
- 配线间和连接线的安全
- 无线网络安全问题
- 无线加密协议(WEP) 和 IEEE 802.11i Beaconing 信标
- MAC 地址过滤
- 汇聚层的安全
- 安全设计举例

第十一课：入侵检测

- 入侵检测的概念
- 基于主机的入侵检测和基于网络的入侵检测
- 识别基于签名和基于网络异常的入侵检测的区别

- 建立入侵检测体系
- 配置和定制 IDS 软件
- IDS 规则
- IDS 的动作与行为
- IDS 的主动审计和被动审计
- 入侵检测软件
- IDS 的选购
- IDS 的更新
- 识别正常的商业行为

第十二课：早期预警

- 早期预警
- 蜜罐技术
- 陷阱技术
- 设置陷阱

第十三课：事件响应

- 编制响应计划
- 建立响应方针
- 提前决定
- 不要惊慌
- 做出正确的行动
- 记录下所有的事情
- 评估当前形势
- 停止和牵制黑客的行为
- 执行响应计划
- 分析和学习
- 创建一个备份计划
- 确定备份计划是完备有效的