网络系统及服务器的应急响应

一、课程描述：

本课程以理论结合实际，讲述了企业风险评估与等保工作、信息安全管理体系建设，以实战实形讲述主机系统安全、服务器安全配置与应急响应，网络系统应急响应、数据库的应急响应以及中间件的应急响应技术，并在课程中介绍了常见的攻击与防范技术。

二、课程大纲：

第 1 讲 网络安全应急响应概述

- 应急响应基本概念
- 网络安全应急响应基本概念
- 网络安全应急响应的能力与方法
- 网络安全应急响应现场处置流程

第 2 讲 企业风险评估与等保工作

- 安全评估基础
- 安全评估实施
- 信息系统审计
- 等保 2.0

第 3 讲 主机系统安全检查与运行维护

- 系统排查
- 进程排查
- 服务排查
- 文件痕迹排查
- 日志分析
- 内存分析
- 流量分析
- 威胁情报

第 4 讲 常用工具介绍

- SysinternalsSuite
- PCHunter/火绒剑/PowerTool
- Process Monitor
- Event Log Explorer
- FullEventLogView
- Log Parser
- ThreatHunting
- WinPrefetchView
- WifiHistoryView
- 应急响应工具箱

第 5 讲 操作系统安全应急响应

- Windows 系统安全加固
- Linux 系统安全加固
- 部署安全的服务器操作系统
- 部署安全的桌面端计算机系统

- 勒索病毒网络安全应急响应
- 挖矿木马网络安全应急响应

第 6 讲 网络系统安全

- 安全检查与运行维护
- 弱点分析与安全检查
- 安全加固与运行维护

第 7 讲 常见的网络攻击安全应响应

- DDoS 攻击网络安全应急响应
- 流量劫持网络安全应急响应

第 8 讲 数据库安全应急响应

- MSSQL 数据库安全
- MySQL 数据库安全
- Oracle 数据库安全

第 9 讲 中间件安全应急响应

- 安全配置 IIS 服务器
- 安全配置 Apache 服务器
- 安全配置 WebLogic

第 10 讲 常见网络服务的安全检查和加固

- Web 服务器加固
- Mail 服务加固
- DNS 服务加固
- FTP 服务加固
- Samba 应用系统加固
- NFS 应用系统加固

第 11 讲 建立信息安全管理体系

- 信息安全管理基础
- 信息安全管理体系建设
- 信息安全管理体系最佳化实践

第 12 讲 密码学及应用技术

- 密码学基础
- 公钥基础设施 PKI
- PKI 体系工作流程
- PKI/CA 技术的典型应用