应急响应实战演练

一、课程描述：

本课程以理论结合实际，讲述了应急响应的流程，并以实战形式讲述Windows\Linux主机检测与响应技术；日志、网络流量、恶意代码等分析技术；最近以案例场景形式讲述勒索病毒、挖矿木马、流量劫持、DDoS攻击、Webshell等网络安全的应急演练。

二、课程大纲：

第1章　应急响应概况

- 应急响应介绍
- 安全事件分类
- 应急响应启动条件
- 应急响应目标
- 应急响应预案制定
- 应急响应一般处置流程

第2章 终端主机检测与响应技术

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

第3章 常用工具介绍

- SysinternalsSuite
- PCHunter/火绒剑/PowerTool
- Process Monitor
- Event Log Explorer
- FullEventLogView
- Log Parser
- ThreatHunting
- WinPrefetchView
- WifiHistoryView

第4章 日志分析技术

- Web日志分析
- Windows\Linux操作系统日志分析
- 网络及安全设备日志分析

第5章 网络流量分析技术

- NetFlow流量分析
- 全流量分析

第6章 恶意代码分析技术

- 恶意代码概述
- Windows 恶意代码分析
- Linux 恶意代码分析
- WebShell 恶意代码分析

第 7 章 勒索病毒网络安全应急响应

- 勒索病毒概述
- 勒索病毒常规处置方法
- 勒索病毒错误处置方法
- 勒索病毒常用响应工具
- 勒索病毒应急实操训练

第 8 章 挖矿木马网络安全应急响应

- 挖矿木马概述
- 挖矿木马常规处置方法
- 挖矿木马常用响应工具
- 挖矿木马应急实操训练

第 9 章 流量劫持网络安全应急响应

- 流量劫持概述
- 流量劫持常规处置方法
- 流量劫持常用响应工具
- 流量劫持应急实操训练（DNS、HTTP、TCP、ARP 劫持排查）

第 10 章 DDos 攻击网络安全应急响应

- DDoS 攻击概述
- DDoS 常规处置方法
- 流量劫持应急实操训练

第 11 章 Webshell 网络安全应急响应

- Webshell 概术
- 常规处置技术
- 常用工具
- Webshell 应急实操训练