CSNA-E 网络分析体系认证

课程目标：

随着互联网的快速发展和信息化程度的不断提高，互联网深刻影响着政治、经济、文化等各个方面，保障信息安全的重要性日益凸显，加强对互联网上各类信息的管理应引起高度重视。在系统安全方面，以提高防御、应急处置能力为主的传统安全管理已经不能适应新计算、新网络、新应用和新数据为新特征的信息安全产业发展的需要。

网络信息安全是一个关系国家安全和主权、社会稳定、民族文化继承和发扬的重要问题。其重要性，正随着全球信息化步伐的加快越来越重要。网络信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。它主要是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

CSNA-E 培训课程表		
日期	课程安排	内容简介
第一天	1. 自报家门 CSNA 体系介绍	CSNA-E 简介
		CSNA-S 简介
		CSASE 简介
	2. 开宗明义 全流量分析技术	全流量分析技术介绍（RAS）
		全流量分析技术的安全运维价值（TSA）
	3. 小试牛刀 实验：全流量分析	实验：RAS 系统的使用
		实验：利用 RAS 找出流量突发时段的大流量主机
	4. 更进一步 通过全流量看新环境下的运维	业务规模发展给传统运维模式带来的挑战
		全流量分析助力新环境下的运维（UPM）
	5. “层”次分明 TCP/IP 架构	TCP/IP 层次模型
		数据包的封装与解封装

	6. 庐山“帧”面目 二层协议解码	二层数据帧深度解码
		实验：通过 16 进制分辨数据帧内容
		众里寻他：ARP 协议的来龙去脉
		以假乱真：ARP 攻击
		案例：如何找出 ARP 欺骗造成的网络攻击
		实验：分析 ARP 攻击行为
第二天	7. “包”罗万象 三层协议解码	IPv4 包头字段解码
		案例：PING 大包丢包故障
		案例：如何发现大型网络中网络环路问题
		实验：分析 3 层环路
		IPv6 包头字段解码
		青鸟传信：ICMP 协议的前世今生
		实验：IPv6 Traceroute 流量分析
第三天	8. “段”章取义 四层协议解码	TCP 协议报头及特点
		TCP 建立连接过程分析
		TCP 断开连接过程分析（半关闭）
		TCP 连接状态机
		案例：电信线路访问招聘网站页面显示故障分析
		案例：设备 MTU 配置错误案例分析
		利用三次握手分析网络时延
		实验：通过三次握手分析网络时延

		TCP 传输机制
		TCP 差错控制
		TCP 拥塞控制
		TCP 分析指标讲解
		案例：解决两台存储之间数据同步失败的问题
		实验：通过 TCP 相关指标判断网络是否存在异常
		UDP 协议头部字段解码
		实验：分析 UDP 协议流量
第四天	9. 楼台亭阁 七层协议解码	HTTP 基本原理
		HTTP 交易解析
		实验：HTTP 请求分析
		HTTPS 基本原理
		实验：手动恢复 HTTPS 证书文件
		DHCP 基本原理
		实验：DHCP 流量分析
		DNS 基本原理
		实验：DNS 流量分析
		邮件协议基本原理
		实验：邮件流量分析
		FTP 基本原理
		实验：FTP 传输过程分析

	10. 独具慧眼 如何准确定位与研判网络攻击	网络扫描原理
		实验：扫描流量分析
		DoS 攻击原理
		实验：分析 DoS 攻击流量
		实验：分析 SQL 注入行为
		木马、蠕虫、僵尸网络简介
		实验：通过流量还原木马样本并分析木马行为
	11. 融会贯通 网络分析方法总结	分析方法总结
		分析场景举例与疑难故障分析流程
	12. 金榜题名 CSNA-E 认证考核	笔试考试（60min）
		数据包分析考试（120min）

CSNA-E 培训课程表