工 业 和 信 息 化 部
电子工业标准化研究院培训中心

电标培〔2024〕013 号

关于举办“网络安全关键技术分析与攻防实践”专题培训班的通知

各有关单位：

随着社会网络化、数字化、智能化进程的不断加速和线上业务的常态运行，以及 AI、5G、大数据、云计算等新技术新应用加速迭代，网络和各类系统在架构、应用等更加多样复杂，由此带来的网络安全风险、威胁、对抗不断升级，也为网络安全攻防手段和有效管理提供了新的技术和需求思路。

因此，持续更新网络安全关键技术知识，提升关键基础设施网络安全防范能力，满足网络环境不断演进的安全需求，已经成为安全从业人员的重要工作。为协助各单位培养“知攻善守”的新时代网络安全技术人才，提升安全事件分析和从攻击中快速恢复的应急处置实战能力，有效保障系统的安全运行，我中心决定举办 “网络安全关键技术分析与攻防实践专题培训班”，现将相关事宜通知如下：

一、培训主要内容（详见附件二）：

第一模块：网络安全法规与标准综述

第二模块：网络安全关键基础技术分析

第三模块：网络安全威胁和攻击技术实践

第四模块：网络安全防护与应急响应

二、培训时间地点：

第一期2024年3月21日—25日课时三天（21日报到） 广州

第二期 2024年3月27日—31日课时三天 （27日报到） 北京

第三期2024年4月9日—13日课时三天 （9日报到） 成都

三、参加对象：

政府及企事业单位、运营商、城市公共服务、公安、银行、医院、民航、能源系统、信息科技公司等机构的网络安全管理、运营和技术实施等相关人员。

四、师资及培训方式：

培训班拟邀请具有实战经验的资深专家教授，以面授讲座、互动交流、答疑解惑相结合的方式进行，并突出理论与实践相结合、案例分析与行业应用相穿插、讲师技术解析和实践演示与学员实操验证相辅助，注重实效。

五、颁发证书：

参加人员完成培训，经考评合格者，由我中心统一颁发专业人员培训证书（请提交二寸白底彩色电子照片至邮箱，像素 358 *441，分辨率350dpi，格式 JPG，照片命名：姓名+身份证号.JPG）。

六、培训费用：

培训费用为3800元/人（含授课费、教材资料费、场地费等）；食宿统一安排，费用自理。

七、报名联系：

本次培训会务工作由北京久阳时代文化交流发展中心具体承办。请参报名人员将加盖单位印章的报名回执表传真或邮件至报名处。

联 系 人：韩老师　　吴老师　　张老师

报名电话：（010）62720486　　62720535　　64102658

传　　真：（010）62720176

E—mail ： jysd18@163.com

培训具体报到通知将发至学员报名邮箱，详告具体报到地点、乘车路线、食宿安排等事宜。

附件一：报名回执表

附件二：课程安排表

工业和信息化部电子工业标准化研究院

培训中心

2024 年 1 月 3 日

附件一：

网络安全关键技术分析与攻防实践专题培训班报名回执表

经研究，选派下列同志参加学习：

单位名称					
详细地址				邮 编	
联 系 人		电 话		传 真	
培训费用	到会支付（　　）对公电汇支付（　　） 刷公务卡（　　）				
姓　名	性别	职务	手 机	E－mail	培训地点
您想了解或希望解决的主要问题：			是否需要安排住宿： （　　）是　　（　　）否		

注：本表复印有效　传真：010-62720176

附件二：

网络安全关键技术分析与攻防实践专题培训班课程安排表

模块	课程内容	演示与实验
网络安全法规与标准综述	➢ 国内网络环境与安全现状介绍 ➢ 网络安全相关法律法规重点解读 网络安全法介绍 数据安全法介绍 关键信息基础设施安全保护条例介绍 网络安全等级保护制度介绍 ➢ 近期网络安全相关法规、标准及条例介绍	
网络安全关键基础技术分析	➢ 信息安全体系结构分析 ➢ 信息安全基础元素 ➢ 信息安全内容概述 ➢ 网络通信模型各层安全风险分析 ➢ 网络协议安全性分析实例 ✧ IP 协议安全性实例 ✧ ICMP 协议安全性实例 ✧ ARP 协议安全性实例 ✧ DNS 协议安全性实例 ✧ HTTPS 协议安全性实例 ➢ 网络数据包结构及工作原理分析 ✧ 数据封装与分片 ✧ 传输超时与重传 ➢ 网络和系统常用网络故障诊断工具 ➢ 使用协议分析仪进行故障发现和诊断 ➢ 利用网管应用进行网络故障诊断和排除 ➢ 网络运维监控系统介绍 ➢ 智能网络管理系统介绍	➢ 利用协议分析工具实现传输及数据封装验证 ➢ 利用协议分析工具实现数据分片技术验证 ➢ 网络数据报文分析实例 ➢ 网络协议安全性分析实例 ➢ 按需实现数据报文构建、播发及验证分析 ➢ 网络故障发现与诊断实例 ➢ 网络运维监控系统示例
网络安全威胁和攻击技术	➢ 安全攻击的目标及目的 ➢ 网络安全渗透测试步骤及流程 ➢ 网络安全渗透测试的执行标准 ➢ 前期交互工作内容解析 ➢ 信息收集技术介绍与实践 ➢ 漏洞分析及攻击技术 ➢ 口令攻击技术介绍与实践 ✧ 应用口令攻击 ✧ 系统口令攻击 ✧ 服务口令攻击 ✧ Hash 算法攻击 ➢ 社会工程学攻击技术 ✧ 站点钓鱼利用 ✧ 邮件钓鱼利用 ➢ 网络协议攻击技术介绍与实践 ➢ 系统漏洞攻击技术 ✧ CVE-2019-0708 漏洞攻击 ✧ CVE-2021-3156 漏洞攻击 ✧ CVE-2022-0847 漏洞攻击 ✧ CVE-2023-21931 漏洞攻击 ✧ CVE-2023-29300 漏洞攻击 ➢ 应用漏洞攻击技术 ✧ Drupal XSS 漏洞攻击 ✧ JBoss 反序列化漏洞 ✧ Nginx 解析漏洞 ✧ PHP 文件包含漏洞	➢ 主机扫描技术测试 ➢ 网络扫描技术测试 ➢ 网络监听技术测试 ➢ 社会工程学攻击测试 ➢ 网络协议漏洞攻击测试 ➢ 口令攻击示例测试 ➢ 网络钓鱼技术示例测试 ➢ 无线安全攻击示例测试 ➢ Windows 系统漏洞攻击示例 ➢ LInux 系统漏洞攻击示例 ➢ ThinkPHP5 等应用漏洞测试 ➢ 木马攻击技术示例 ➢ Web 暴力攻击示例 ➢ Web 文件上传攻击示例 ➢ SQL 注入漏洞攻击示例 ➢ 提权技术测试 ➢ 中间人场景示例 ➢ 内网代理技术测试 ➢ 内网靶场环境测试 ➢ ……

	✧ ThinkPHP5 远程代码执行漏洞 ➢ 木马攻击技术 ✧ 木马生产技术 ✧ 木马免杀技术 ✧ 木马捆绑技术 ➢ 无线安全攻击技术 ✧ 无线可用性攻击 ✧ 无线认证协议攻击 ✧ 握手包破解攻击 ✧ PIN 码攻击 ✧ 社工方式攻击 ➢ Web 安全攻击技术 ✧ Web 暴力攻击 ✧ 文件上传漏洞攻击 ✧ 命令执行漏洞攻击 ✧ XSS 漏洞攻击 ✧ SQL 注入漏洞攻击 ➢ 提权技术 ✧ 内核提权技术 ✧ 服务提权技术 ✧ Sudo 提权技术 ✧ SUID / SGID 提权技术 ➢ 内网渗透攻击技术 ✧ 中间人场景搭建 ✧ 内网穿透技术介绍 ✧ 内网代理技术 ➢ 安全渗透测试实战演练与过程解析 ➢ 容器安全技术简介 ➢ 云与大数据安全技术简介 ➢ 人工智能安全风险与应对简介 ✧人工智能安全风险的类型 ✧人工智能安全风险的危害及表现 ✧人工智能安全风险的应对策略	
网络安全防护与应急响应	➢ 网络安全防护技术体系架构介绍 ➢ 身份认证技术介绍 ➢ 授权与访问控制技术解析 ➢ 资产保护技术解析 ✧ 数据安全存储 ✧ 数据安全传输 ✧ 数据安全授权 ➢ 病毒与补丁防护 ➢ 系统异常行为的审核与追踪 ➢ 传输安全性保障技术 ➢ 数字证书技术实践及应用 ➢ 系统安全基线规划与设定 ➢ 系统安全防护与加固措施 ➢ 网络设备安全管理 ➢ 网络安全设备的规划与部署 ➢ 安全巡检制度与内容介绍 ➢ 安全运维应急响应介绍 ➢ 应急响应流程与技术举例 ➢ 安全应急响应技术介绍 ➢ 专项应急方案制定	➢ 数据安全性防护示例 ➢ 传输安全性实现测试 ➢ 数字证书体系构建测试 ➢ 数字证书应用实例测试 ➢ 系统安全基线制定与扫描测试 ➢ 系统安全加固实例测试 ➢ 安全巡检脚本制定与测试 ➢ 安全设备的部署、规划与管理 ……

注：此内容可根据学员需求微调，以现场通知为准。