工业和信息化部电子工业标准化研究院

关于举办“红蓝对抗实战演练与入侵溯源分析能力提升”培训的通知

各相关单位:

在AI技术快速发展的时代背景下，红蓝对抗向自动化趋势演进，黑客攻击重心向内网渗透发展。新技术不断迭代导致网络犯罪呈现新的特征。如何从技术上设关布阵实现层层防护，成为企事业网络安全红蓝队专家和骨干必须掌握的关键技能。

为帮助各企事业单位储备一批政治和技术都过硬的技术骨干人才，从HW演练开始，研讨如何真正防住黑客，提高人员的攻防打点和内网渗透技能。工业和信息化部电子工业标准化研究院定于2025年9月14日-17日在北京举办“红蓝对抗实战演练与入侵溯源分析能力提升”培训班。具体安排如下:

一、培训对象

培训对象为红蓝队人员、网络安全技术人员、系统管理员、网络管理员、应用管理员和数据管理员等企事业单位骨干技术人员，涉及到企事业一线网络安全技术建设、安全运营、网络与数据安全管理、规划设计、部署实施、优化改进相关工作。

二、培训形式、时间和地点

本次培训采用面授方式开展，课程中组建红队和蓝队，利用

攻防对抗方式，结合对抗演练方式，推演与研讨如何更好地开展各自的对抗备战工作。

培训时间：2025 年 9 月 14 日-9 月 17 日（14 日全天报到）

培训地点：北京，具体地点详见《报到通知》

会务组将于开班前一周将《报到通知》发给各参培学员，详细报到地点、乘车路线、食宿及日程安排等事宜。

三、培训内容

（一）蓝队必备—HW前期自查工作要点

1. HW常规入侵思路

① 跨分支机构/服务商单位渗透思路

② 跨公有云/私有云/社区云/虚拟化平台渗透思路

③ 综合社会工程学渗透思路

④ 内网渗透思路和路线

⑤ 往年 HW 被打穿案例分析

2. HW常用攻击手段

① HW 常用外部突破手段

② HW 常用内网渗透手段

3. HW前期自查工作清单

4. HW前期自查工作要点

① 网络安全架构如何分析

② HW 保障资产如何梳理

③ 如何全面基础安全自查

④ 业务系统如何风险分析

⑤ 内部账号如何安全审计

⑥ 安全能力缺陷如何补充

⑦ 整体安全策略如何优化

⑧ 发现风险如何整改推进

（二）蓝队必备—HW资产梳理实战指导

1. 资产梳理的重要性及作用有哪些

2. 资产梳理都应该做什么

3. 怎么做资产梳理

① 资产梳理方法和流程如何制定

② 资产梳理工作难点及解决方法有哪些

4. 漏洞扫描如何实施好

① 怎么做安全漏洞扫描

② 怎么更好地评估漏洞扫描结果

③ 如何处理误报和漏洞问题

（三）蓝队必备—网络安全防护分析与如何快速入侵应急响应

1. 网络安全防护分析

① 如何做好深度安全防护效果分析

② 网络安全域设计和访问控制如何分析

③ 域间访问控制矩阵如何设计和安全确认

④ 防火墙规则设计有效性如何评价

⑤ 安全设备配置规则有效性如何评价

⑥ 日志管理和警报能力如何评价

2. 系统加固实践

① 操作系统如何做好加固

② 数据库如何做好加固

③ 中间件如何做好加固

④ 常见加固遇到的难题和如何处理

3. 入侵应急响应

① HW 中常见安全事件有哪些

② 常见攻击思路对应的快速应急思考

③ 如何开展快速分析与侦查

④ 常用分析工具有哪些？如何使用

⑤ 如何开展取证工作

4. 安全事件闭环管理

① 安全事件闭环管理流程如何全面开展

② 如何提高安全事件处理规范性及效率

③ 如何协调各方团队资源开展事件处置

（四）红队视角看溯源—信息收集、指纹检测【红队平台 KALI】

1. 指纹识别原理

2. 指纹检测攻击实践

3. Banner获取版本

4. HTTP协议指纹探测

5. HTTP指纹探测防范方法

（五）红队视角看溯源—SQL注入漏洞利用与防范实践【红

队平台KALI】

1. SQL注入发现与利用思路

2. 手工SQL注入获取数据库信息

3. 手工提取用户和密码信息并破解

4. 常见SQL注入漏洞利用工具使用实践

5. SQL注入漏洞代码修补实践

6. SQL注入漏洞修补后攻击绕过

（六）红队视角看溯源—跨站入侵分析与防范实践【红队平台KALI】

1. XSS漏洞原理与漏洞发现方法

2. 利用XSS在后台增加管理员账户

3. 利用XSS实现钓鱼攻击

4. XSS脚本利用平台

5. CSRF高级脚本入侵分析与实践

6. XSS漏洞修补、CSRF漏洞修补

（七）红队视角看溯源—文件上传漏洞利用与后门连接【红队平台KALI】

1. 上传漏洞利用实践、上传漏洞监控检测、上传漏洞利用思路、上传漏洞防范解析

2. 后门连接创建攻击实践、后门连接本地监听、后门连接反向连接、后门连接监控检测实践、后门连接防御

3. 系统权限提升、后门 Rootkit安装与检测、后门计划任务方式植入、黑客系统入侵痕迹清除与发现、ARP欺骗与网络流

量监听

（八）综合入侵与防御对抗实战演练一【1 红队打点与内网渗透 2 蓝队溯源分析实践】

1. 外部网站入侵过程重现

① 打点漏洞发现

② 打点漏洞利用

③ 网站挂马与扩张

④ 内网渗透与隧道建立

2. 外部网站入侵侦查分析

① 客户端系统控制过程分析

② 网站入侵过程分析

③ 数据库入侵分析过程分析

3. 网站挂马入侵应急响应

① 网站应急处置与加固

② 数据库应急处置与加固

③ 客户端系统应急处置与加固

（九）综合入侵与防御对抗实战演练二【1 红队打点与内网横向移动 2 蓝队溯源分析实践】

1. 信息收集渗透突破口

2. 后台管理地址扫描不成功如何深入开展

3. 对管理后台抓包并发起字典攻击，字典破解不成功，如何社工构造字典攻击成功

4. 如何发现和利用Web网站任意代码执行漏洞上传

Webshell

5. 如何绕过Web网站限制新增超级权限用户

6. 如何在内网横向扫描并进行内网信息探测

7. 如何搭建隧道绕过防火墙，创建代理并利用HTTP进入目标内网

8. 如何攻击内网数据库服务器并实现隧道远控

9. 如何利用Redis服务器漏洞隧道反连到黑客机并增加后门账号

10. 如何进一步突破内网业务Web服务器并实现提权及远控脱裤

四、证书颁发

考试合格者，由工业和信息化部电子工业标准化研究院统一颁发《入侵溯源分析》专业技术人员培训证书。证书查询网址：www.cesi.cn。

五、培训费用

培训费：6900元/人（含师资、教材、证书、辅导、三天午餐），住宿统一安排，费用自理。

六、缴费须知

单位名称：启强赐恒科技（北京）有限公司

开 户 行：中国农业银行股份有限公司北京房山城关支行

汇款帐号：1110 0101 0400 23694

汇款附言： 入侵溯源分析培训费（姓名、单位）

七、联系方式

此次培训工作将由启强赐恒科技(北京)有限公司具体承办，请参加培训的学员认真填写报名回执表，以电话、传真及邮件的方式反馈至我单位。

电　话：010-53397598　　010-64102658

联系人：田 悦　　刘老师

联系邮箱：2021411678@qq.com

附件：报名表

工业和信息化部电子工业标准化研究院

2025 年 8 月 1 日

附件

《红蓝对抗实战演练与入侵溯源分析能力提升》培训班报名表

<table>
<tr><td>单位名称</td><td colspan="3"></td><td rowspan="5">电子版照片</td></tr>
<tr><td>姓 名</td><td></td><td>性 别</td><td></td></tr>
<tr><td>部 门</td><td></td><td>职 务</td><td></td></tr>
<tr><td>最高学历</td><td></td><td>毕业院校</td><td></td></tr>
<tr><td>手 机</td><td></td><td>身份证号</td><td colspan="2"></td></tr>
<tr><td>电子邮箱</td><td></td><td>通讯地址</td><td colspan="2"></td></tr>
<tr><td>培训地点</td><td colspan="4">北京 9 月 14 日-17 日（14 日报到）</td></tr>
<tr><td>发票类型</td><td colspan="2">□增值税普通发票</td><td colspan="2">□增值税专用发票</td></tr>
<tr><td>开票项目</td><td colspan="4">培训费□ 会议费□ 资料费□ 技术服务费□</td></tr>
<tr><td colspan="5">增值税发票开票信息（以提供信息为准，确保无误）</td></tr>
<tr><td>单位名称</td><td colspan="2"></td><td>纳税人识别号</td><td></td></tr>
<tr><td>地 址</td><td colspan="2"></td><td>电 话</td><td></td></tr>
<tr><td>开户行</td><td colspan="2"></td><td>账 号</td><td></td></tr>
<tr><td>汇款账号</td><td colspan="4">户 名： 启强赐恒科技（北京）有限公司
开 户行： 中国农业银行股份有限公司北京房山城关支行
账 号： 1110 0101 0400 23694</td></tr>
<tr><td colspan="2">是否住宿： □是 □否
预定房间数量（ ）</td><td colspan="3" rowspan="2">单 位 印 章
日期：2025 年 月 日</td></tr>
<tr><td colspan="2">注：各参培人员请在报名 3 日内将相关费用通过银行等方式付款，会务组确认到款后，统一开具发票。</td></tr>
<tr><td colspan="5">联 系 人：田 悦 18511991911 （同微信）
联系电话：010-53397598 传真：010-53397598
邮 箱：2021411678@qq.com</td></tr>
</table>