附件1：

# **网络空间安全公益讲师**

# **认证材料**

## 一、认证对象

已取得网络空间安全公益讲师认证资格的讲师或正在等待认证的讲师。

## 二、课程要求

### （一）课程范围

见附件2

### （二）课程形式

1．提供视频课程：视频需画质清晰、声音流畅，内容生动有趣，适合线上学习。

2．提供PPT与课程脚本：PPT设计需简洁明了，脚本内容详实、逻辑清晰。

3．只提供PPT：PPT内容需完整、有条理，能够清晰传达核心知识点。

4．只讲解他人PPT：讲解需结合自身理解，语言流畅，确保内容准确无误。

### **（三）课程质量**

1．内容准确科学：课程内容需基于网络安全领域的最新研究成果和实践经验，确保信息的权威性与准确性。

2．语言清晰易懂：语言表达需简洁明了，避免过度使用专业术语，适合不同层次的受众理解，让网络安全知识“飞入寻常百姓家”。

3．设计合理完整：课程需有明确的教学目标、合理的结构安排和有效的教学方法，能够有效传达核心知识点，激发学习者的学习兴趣。

### **（四）课程时长**

单个课程时长为1-45分钟。课程需在有限的时间内，内容充实、重点突出，能够高效传递核心知识点，避免冗长拖沓。

### **（五）课件呈现**

讲师可采用组委会所提供的PPT模板，亦可自行设计制作演示文稿，但必须在演示文稿中嵌入指定的LOGO。



### **（六）公益时长认定**

1．提供视频课程的讲师，视频时长将1:1换算为年度公益宣讲时长。

2．提供PPT与课程脚本的讲师，按视频时长的50%换算年度公益宣讲时长。

3．只提供PPT的讲师，按最终拍摄视频时长的30%换算年度公益宣讲时长。

4．只讲解他人PPT的讲师，按视频时长的50%换算年度公益宣讲时长。

5．按录制视频提供课程内容的练习题（单选、多选、判断题），每5道练习题可换算半小时的公益宣讲时长。

## 三、参与方式

### d8094cbe76ff564b404dc642c17d7c0（一）报名方式：请扫码下方二维码，选课报名

### （二）课程提交

报名后，公益讲师按照要求录制或准备课程，并在选课后的15天内将课程文件（视频、PPT、脚本等）命名为“姓名+课程名称”发送至wal\_zyfw@163.com。

附件二：

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **级别** | **培训基础** | **总课时** | **培训课程** | **培训目标** | **课时** | **小程序选项** | **详细内容** | **备注** | **考试分值** |
| 一 | 具备普通高校入学条件，且高考科目含物理。 | 26 | 爱国教育 |  | 1 |  | 爱国教育、总体国家安全观 |  |  |
| 安全法律基础 | 了解《网络安全法》、《个人信息安全保护法》、《数据安全法》、《国家安全法》、《反间谍法》、《密码法》的基本内容。 | 10 | 《网络安全法》 《个人信息安全保护法》 《数据安全法》 《国家安全法》 《反间谍法》 《密码法》 | 《网络安全法》： 1. 网络安全法的背景 2. 网络安全法的意义 3. 网络安全法的必要性 4. 网络安全等级保护制度 5. 关键信息基础设施保护制度 6. 网络运营者、网络产品和服务提供者义务要求 7. 网络信息安全保障要求 8. 重要数据跨境传输安全要求 9. 网络安全审查制度   《个人信息保护法》： 1. 个人信息和敏感个人信息的定义 2. 去标识化和匿名化的含义 3. 个人信息主体的权利 4. 核心原则：“告知-同意” 5. 个人信息处理“三最原则” 6. APP收集个人信息的要求 7. 针对大型互联网平台采集个人信息的要求 8. 针对大数据杀熟的规定 9. 针对敏感信息的规定 10. 个人信息影响评估活动 11. 违法行为的惩处力度 12. 个人信息保护实践  《国家安全法》 1. 立法背景与目的 2. 国家安全定义 3. 国家安全工作原则 4. 维护国家安全的任务 5. 国家安全保障与公民、组织的义务和权利 6. 法律责任 7. 全民国家安全教育日  《反间谍法》 1. 立法背景与目的 2. 间谍行为的定义 3. 法律的主要内容 4. 法律责任 5. 法律实施的意义与影响  《密码法》 1. 密码及其分类 2. 密码技术产品服务介绍 3. 国产密码算法介绍 4. 密码法介绍 5. 密码相关政策介绍 6. 密码应用方案介绍 7. 密评工作介绍 |  |  |
| 信息安全常识 | 了解常见网络安全威胁（诈骗、病毒、网络攻击、数据窃取、数据篡改、AI仿冒）等； 了解常见的不安全行为及其危害。 保密意识和保密办法。 | 6 | 日常办公安全意识 日常生活安全意识 保密意识培训 | 日常办公安全意识： 1. 电脑口令安全 2. 电脑屏保安全 3. 电脑防病毒和防火墙使用 4. 电子文档加密解密 5. 压缩文件加密解密 6. 邮件安全收发 7. U盘安全使用 8. 防范钓鱼邮件 9. 办公场所安全   日常生活安全意识： 1. APP安全 2. 二维码安全 3. 无线使用安全 4. 手机更换回收安全 5. SIM卡安全使用 6. 移动支付安全 7. 个人隐私保护  保密意识培训： 1. 日常会议保密要求 2. 涉外工作保密要求 3. 对外商务活动保密要求 4. 计算机网络使用保密要求 5. 办公自动化使用保密要求 6. 养成良好的保密工作习惯 | 特色课程 |  |
| 志愿服务通识 | 了解《志愿服务条例》、志愿服务的礼仪规范、网络安全志愿服务的主要形式。 | 3 | 志愿服务通识 | 1、《志愿服务条例》 2、志愿服务的礼仪规范 3、网络安全志愿服务的主要形式 | 特色课程 |  |
| 安全守护者行动常识 | 了解安全守护者行动的组织架构；了解网安联和北京网络空间安全协会的历史和服务；熟悉网安联小程序等相关工具； 熟悉《安全志愿守护者管理办法》。 | 2 | 安全守护者行动常识 | 1、安全守护者行动的组织架构 2、网安联和北京网络空间安全协会的历史和服务 3、网安联小程序等相关工具； 4、解读《安全志愿守护者管理办法》 | 必学课程 |  |
| 逻辑代数 | 熟练掌握逻辑运算方法。 | 4 | 逻辑代数 | 1. 逻辑代数简介 2. 逻辑代数的基本概念 3. 逻辑代数运算规则 4. 逻辑代数表达式 5. 逻辑代数应用 |  |  |
| 二 | 1.高等数学/数学分析、线性代数/高等代数、程序设计（至少掌握一门高级语言）、基础物理、模拟电子技术、数字电路技术； 2.完成级别一课程。 | 34 | 信息论 | 理解信息相关概念。 | 6 | 信息论 | 1.信息论基本概念  2.信息熵与信息量   3.信道容量与信源编码  4.信道编码与解码  5.信息论在实际应用中的发展 |  |  |
| 逻辑学 | 理解常见的逻辑思维 | 3 | 逻辑学 | 1. 命题及推理 2. 归纳法 3. 演绎法 4. 逻辑推理 5. 逻辑思考 6. 逻辑发言 7. 发散性思维 8. 金字塔思维 |  |  |
| 计算机常识、服务器、机房等知识 | 了解计算机的分类、主要软硬件组成及其功能。 | 5 | 计算机常识 服务器知识 机房知识 | 1. 计算机组成架构 2. 服务器的特点 3. 塔式服务器 4. 机架服务器 5. 刀片服务器 6. 超融合服务器 7. NAS、DAS、SAN介绍 8. RAID介绍 9. 服务器日常监控及管理 10. 服务器带外管理网络 11. 机房物理安全环境（监控、门禁、防火、防水、防雷、防静电、电磁屏蔽等） |  |  |
| 操作系统及其安全基础 | 了解操作系统分类及其代表产品、操作系统基本原理，熟悉常见系统的安全漏洞和应对方法。 | 12 | Windows安全 Linux安全 | Windows安全： 1. Windows 的基本概念和术语 2. Windows 系统架构 3. Windows 安全体系结构 4. Windows 身份认证机制 5. Windows 授权与访问控制机制 6. Windows 安全审计机制 7. Windows 磁盘加密 Bitlock 8. Windows 日志分析 9. Windows 安全加固 10. Windows Sysinternals 工具介绍  Linux安全： 1. Linux的安全架构 2. Linux的身份认证机制 3. Linux的授权与访问控制机制 4. Linux的安全审计机制 5. Linux的SELinux介绍 6. Linux的iptables防火墙 7. Linux的日志分析 8. Linux的安全加固 |  |  |
| 志愿服务实践 | 待定 | 8 | 志愿服务实践 | 志愿服务实践 | 特色课程 |  |
| 三 | 1.数据结构、通信原理； 2.完成级别二课程。 | 36 | 网络原理和常识 | 熟悉网络类型、IP地址版本和分类、OSI 7层协议架构，各层代表性协议，数据交换原理； 了解常见的网络设备。 | 15 | 计算机网络原理和协议安全 | 1. OSI网络模型介绍 2. TCP/IP网络模型介绍 3. TCP/IP网络协议栈安全缺陷与攻击技术 4. 用Wireshark分析TCP三次握手 5. 用Wireshark分析HTTPS协议 6. IP源地址欺骗 7. ARP欺骗 8. DNS安全 9. TCP SYN Flood拒绝服务攻击 10. UDP Flood拒绝服务攻击 11. 工控网络架构介绍 12. 物联网网络架构介绍 13. VMWare虚拟机的使用 14. VMWare虚拟机虚拟网络NAT、桥接、仅主机模式介绍 15. 交换机、路由器介绍 |  |  |
| 信息安全基础 | 信息安全分类； 保密性、完整性、不可否性、可控性、可靠性的概念和保证机制。 | 6 | 信息安全基础 | 1. 信息化发展状况 2. 当前信息安全问题 3. 当前网络安全态势 4. 网络空间安全的内涵和外延 5. 我国网络空间安全战略 6. 保密性 7. 完整性 8. 可用性 9. 真实性、可核查性、抗抵赖性、可靠性 10. 信息安全发展阶段（通信安全阶段、计算安全阶段、信息系统安全阶段、信息安全保障阶段、网络空间安全阶段） 11. 信息安全问题的根源（内因、外因） 12. 信息安全的特征（系统性、动态性、无边界性、非传统性） 13. 常用的信息安全保障模型（IPDRR、IATF、ASA、滑动标尺模型、STRIDE、WPDRRC、ATT&CK、Cyber Kill Chain等） |  |  |
| 网络安全法规和规范 | 了解《网络安全等级保护条例》、《信息安全风险评估方法》、《个人信息安全规范》、《关键信息基础设施安全保护要求》、《互联网信息服务管理办法》； | 5 | 《网络安全等级保护条例》 《信息安全风险评估方法》 《个人信息安全规范》 《关键信息基础设施安全保护要求》 《互联网信息服务管理办法》 | 《网络安全等级保护条例》 1. 立法背景与依据 2. 适用范围与对象 3. 主要内容与要求 4. 实施意义与影响  《信息安全风险评估方法》 1. 风险评估框架及流程 2. 风险评估实施过程 3. 风险识别 4. 风险分析 5. 风险计算 6. 风险评价 7. 报告编写   《个人信息安全规范》 1. 个人信息安全基本原则 2. 个人信息的收集 3. 个人信息的存储 4. 个人信息的使用 5. 个人信息主体的权利 6. 个人信息的委托处理、共享、转让、公开披露 7. 个人信息安全事件处置 8. 组织的个人信息安全管理要求  《关键信息基础设施安全保护要求》 1. 关基保护的基本原则 2. 分析识别 3. 安全防护 4. 检测评估 5. 监测预警 6. 主动防御 7. 事件处置 8. 关基保护方案介绍  《互联网信息服务管理办法》 1. 立法背景与目的 2. 适用范围与对象 3. 主要内容与要求 4. 法律责任 5. 实施意义与影响 |  |  |
| 网络内容安全 | 熟悉内容安全类别、内容审核方法。 | 4 | 网络内容安全 | 1. 网络内容安全面临的挑战 2. 维护网络内容安全的措施 3. 网络内容安全审核方法 4. 网络内容安全相关政策文件介绍 |  |  |
| 等保定级与等保测评 | 等保定级的流程； 等保测评的工作内容和方法，报告编制； | 6 | 等保定级与等保测评 | 1. 等级保护2.0 背景介绍和相关法规政策体系介绍 2. 等级保护2.0 整体框架介绍 3. 等级保护2.0 整体实施流程介绍 4. 等级保护2.0 系统定级方法 5. 等级保护2.0 系统备案方法 6. 等级保护2.0 基本要求解读 7. 等级保护2.0 技术体系结构设计 8. 等级保护2.0 管理体系架构设计 9. 等级保护2.0 扩展安全技术体系设计（云计算、物联网、大数据、移动互联、工控系统） 10. 等级保护2.0 实践案例 | 特色课程 |  |
| 四 | 1.离散数学、概率论与数理统计、信息安全数学基础； 2.完成级别三课程。 | 39 | 密码学基础 | 了解密码学相关知识并初步具备使用密码加解密等技能，包括编码解码、古典密码学、RSA、AES、DES、SM2、SM4现代密码学算法、量子密码学等。 | 16 | 密码学基础 | 1. 密码学的发展阶段 2. 保密通信模型 3. 密码体系安全性 4. 科克霍夫准则 5. 对称密码算法 6. 非对称密码算法 7. 哈希函数 8. 消息认证码 9. 数字签名 10. 公钥基础设施 11. 国密算法介绍（SM1、SM2、SM3、SM4、SM7、SM9） 12. 密码加密、解密、数字签名演示 |  |  |
| 数据库及其安全 | 了解数据库系统、掌握基本的SQL命令；了解常见的数据库安全问题。 | 10 | 数据库及其安全 | 1. 数据库基本概念 2. 常用的SQL语句 3. 数据库安全性概述 4. 数据库安全性控制 5. 数据库视图机制 6. 数据库审计 7. 数据库加密机制 8. 数据库完整性机制 9. 数据库可用性机制 |  |  |
| 数据资产和数据安全 | 大数据概念； 数据资产常识和相关政策； 数据的合规利用； 数据脱敏、数据隐藏技术； | 4 | 数据资产和数据安全 | 1. 大数据概述 2. 大数据的特点（4V） 3. 大数据安全问题 4. 数据脱敏技术 5. 数据隐藏技术 6. 数据水印技术 7. 数据删除技术 8. 大数据产业政策介绍 9. 大数据合规利用 | 特色课程 |  |
| 软件安全开发基础 | 了解软件开发模型、典型不安全编码和函数使用行为、SDL和DevOpsSec等软件安全开发模型。 | 3 | 软件安全开发基础 | 1. 常用的软件安全开发模型介绍（微软SDL、CLASP、BSI、SAMM） 2. 威胁建模介绍 3. 软件安全需求 4. 软件安全设计原则（最小特权原则、最小特权原则、默认故障处理保护原则等） 5. 软件安全实现 6. 攻击面分析和收敛 7. 通用编码原则 8. 软件安全测试（白盒、黑盒、灰盒） 9. 软件安全交付 10. 软件供应链安全管理 11. DevSecOps介绍 | 特色课程 |  |
| 安全管理与安全审计 | 熟悉信息安全管理理论和管理要求； 熟悉审计制度和方法。 | 4 | 安全管理与安全审计 | 1. 信息安全管理体系概述 2. 信息安全策略与标准 3. 信息安全管理体系实施与运维 4. 信息安全管理体系的审计与认证 5. ISO 27001标准体系介绍 6. ISO 20000标准体系介绍 7. 信息安全管理机构建立 8. 信息安全管理制度体系建立 9. 信息安全管理人员职责划分 10. 信息安全管理的最佳实践 | 特色课程 |  |
| 信息技术应用创新常识 | 了解信创背景、相关政策、技术路线、生态和市场情况。 | 2 | 信息技术应用创新常识 | 1. 信创产业生态体系介绍 2. 信创产业相关政策介绍  3. 信创安全问题研究与网络产品安全漏洞管理规定解读 4. 信创CPU、操作系统、中间件、数据库体系介绍 5. 信创市场情况介绍 6. 信创集成技术介绍 | 特色课程 |  |
| 五 | 完成级别四课程。 | 45 | 计算机病毒、恶意代码及其应对 | 了解病毒和恶意代码原理、熟悉常见的病毒类型和典型病毒，了解病毒和恶意代码的防范原理、查杀方法和常用工具。 | 6 | 恶意代码分析及防范 | 1. 恶意代码概述 2. 恶意代码分类 3. 恶意代码发展简史 4. 病毒、后门、木马、蠕虫、脚本介绍 5. APT介绍 6. 挖矿木马介绍 7. 勒索病毒介绍 8. 移动恶意代码介绍 9. 主机防病毒技术介绍 10. 网络防病毒技术介绍 11. 恶意代码分析工具介绍 12. 企业级防恶意代码解决方案 |  |  |
| 网络攻防原理 | 网络攻击的常规思路、常用方法、常见工具,以及针对攻击的网络防御方面常规的防御思路、防御工具。 红蓝对抗模式与CTF比赛技巧。 | 12 | 网络安全攻防 CTF培训 | 网络安全攻防： 1. 网络信息收集技术 2. Web信息搜索与挖掘 3. DNS与IP查询 4. 网络拓扑侦察 5. 开源情报收集OSINT 6. 漏洞扫描和端口扫描 7. 缓冲区溢出攻击 8. Web浏览器安全攻防 9. 内网渗透 10.常用工具介绍（Nmap、Nessus、Burpsuite、Metasploit、浏览器与插件、Kali）  CTF培训： 1. CTF赛事介绍 2. 常见的编码与解码算法 3. 入门：Web篇 4. 二进制安全：PWN篇 5. 加密解密：Crypto篇 6. 移动安全：APK篇 7. 信息隐写 8. 流量分析 9. 计算机取证 10.文本、视频、二维码分析 |  |  |
| 网络安全设备运维和安全服务 | 掌握常见网络安全设备类型、原理和功能。 了解防火墙、IDS、IPS、堡垒机等的运维，以及常见的安全服务实施。 | 12 | 网络安全设备运维和安全服务 | 安全运维和安全服务介绍： 1. 防火墙原理和使用 2. IDS/IPS原理和使用 3. WAF原理和使用 4. 堡垒机原理和使用 5. 基线核查服务 6. 漏洞扫描服务 7. 安全托管服务 8. 应急响应服务 9. 渗透测试服务 10. 安全日志分析服务 11. 威胁溯源服务 12. 重保值守服务 13. 安全服务项目实施流程 | 特色课程 |  |
| 漏洞扫描和渗透测试基础 | 了解常见的漏洞； 初步具备常用WEB安全检测及对抗技术、漏洞挖掘与利用技术手段等技能。 | 8 | 渗透测试基础 | 1. Web安全简介 2. HTTP请求流程 3. SQL注入漏洞 4. XSS漏洞 5. 上传漏洞 6. 命令执行漏洞 7. CSRF 漏洞 8. 代码注入 9. 旁注攻击 10. 暴力破解 11. 失效的验证和会话管理 12. 不安全的对象直接引用 13. 不安全的配置管理 14. 不安全的密码存储 15. 错误的访问控制 16. 传输保护不足 17. 未经验证的网址重定向 18. 不恰当的异常处理 | 特色课程 |  |
| 网络安全职业发展指引 | 安全守护者行动岗位与职责介绍； 职业发展规划和职称升级路径； 求职技巧。 | 2 | 网络安全职业发展指引 | 1. 如何认识自己 2. 如何提高硬实力 3. 如何打造软实力 4. 如何成为领域专家 5. 时间管理与精力管理 6. 参加校内外实践 7. 明确自己的发展方向 8. 大学的考试与证书 9. 简历如何编写 10. 面试问答技巧 11. 平稳度过职场新手期 | 特色课程 |  |
| 信息安全产业生态 | 了解信息安全的代表性产品、主流厂商和市场状况。 | 2 | 信息安全产业生态 | 1. 信息安全产业生态 2. 信息安全主流安全厂商介绍 3. 信息安全主流产品类型介绍 4. 信息安全主流安全服务介绍 5. 信息安全新领域新赛道介绍 | 特色课程 |  |
| 人工智能及其安全 | 图像与信息隐藏技术； AI相关伦理与认知安全； 生物识别安全。 AIGC | 3 | 人工智能及其安全 | 1. 人工智能基本概念 2. 人工智能产业生态 3. 人工智能安全风险 4. 人工智能相关政策和标准 5. 大模型LLM安全风险 6. 人工智能增强威胁检测 7. 人工智能辅助安全运营 8. AIGC安全介绍 | 特色课程 |  |
|  | 合计课时 | 180 |  |  |  |  |  |  |  |