

# 团体标准《网络空间安全专业人员能力评价 第1部分：渗透测试》编制说明

## 一、工作简况

### 1.1 任务来源

《网络空间安全专业人员能力评价 第1部分：渗透测试》由网安联认证服务有限公司作为提出单位。该标准由广东省网络空间安全协会归口管理。

### 1.2 主要起草单位和工作组成员

本标准由广东省网络空间安全协会牵头，山石网科通信技术股份有限公司、广东电网有限责任公司、韶关学院、广东省科技基础条件平台中心、网安联认证服务有限公司、广州华南信息安全测评中心等多家单位共同参与编制。

### 1.3 主要工作过程

(1) 2021年5月，《网络空间安全专业人员能力评价 第1部分：渗透测试》团体标准立项，随后对外征集参编单位，并组织参与本标准编写的人员召开会议，成立标准编制小组，确立各自分工，进行初步设计，并听取各协作单位的相关意见。

(2) 2021年6月，经多次研讨并参考各类国家标准和相关政策文件，形成标准草案第一稿，后期经内部多次讨论研究，形成第二稿。

(3) 2021年7月，基于前期成果，经多次内部讨论研究，组织标准编制人员完善草案内容，形成征求意见稿。

## 二、标准编制原则和标准编制详细说明及解决的主要问题

### 2.1 编制原则

本标准的研究与编制工作遵循以下原则：

#### (1) 符合性原则

本标准符合法律法规和强制性标准要求，不损害人身健康和生命财产安全、国家安全、生态环境安全，符合国家相关主管部门的要求。

#### (2) 实用性原则

本标准规范是对实际工作成果的总结与提升，保持整体结果合理且维持原意和功能不变，针对不同的用户群体，做到可操作、可用与实用。

### 2.2 文档结构

《网络空间安全专业人员能力评价 第1部分：渗透测试》标准文档分为前言、范围、规范性引用文件、术语和定义、认证级别、认证方式、人员基本要求、直接认证、鉴定认证等部分。

### 2.3 整体格式

整体格式根据 GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的相关要求，对本标准的各要素进行编写和排版。

在标准内容汇总过程中，对各编写组成员提交过来的部分，根据 GB/T 1.1-2020 的编写要求进行了必要的增删改，以确保符合一致性、协调性、易用性等文件的表述原则及相关规定。

### 2.4 标准名称英文翻译

标准的名称“网络空间安全专业人员能力评价第1部分：渗透测试”翻译为 Competence Evaluation of Cyberspace Security Professionals Part 1: Penetration Testing。

## 2.5 术语和定义

术语和定义中所列的术语的英文翻译，根据各部分编写成员提供的术语，如有类似术语的标准，参考了其翻译，没有类似术语标准翻译的，通过百度翻译和谷歌翻译后进行对比，并参考网络相关翻译后进行确定。

## 2.6 认证级别

本章主要阐述了网络空间安全渗透测试人员等级分类情况。渗透测试人员共设三个等级，分别为：渗透测试一级（初级）人员、渗透测试二级（中级）人员、渗透测试三级（高级）人员。

## 2.7 认证方式

本部分介绍了网络空间安全渗透测试人员的认证方式，包括直接认证和鉴定认证。在地级以上市举办的网络安全攻防与应急实战演练、CTF 竞赛、职业技能竞赛、其它重大创新竞赛或演练等相关活动中获得荣誉或奖项的，可根据获奖情况直接对其进行认证。否则，渗透测试人员需经过专业技能培训方可进行鉴定认证。

## 2.8 人员基本要求

本部分主要阐述了网络空间安全渗透测试人员应满足的基本要求，包括具有独立的民事行为能力，具备承担法律责任的能力；无违法犯罪记录；不存在法律法规禁止从业的情形；自愿遵守颁布的渗透

测试人员认证相关文件的有关规定，履行相关义务等。

## 2.9 直接认证

直接认证是指在地级以上市举办的网络安全攻防与应急实战演练，CTF 竞赛，职业技能竞赛，其它重大创新竞赛或演练等相关活动中获得荣誉或奖项的，可根据获奖情况直接对其进行认证。认证等级根据渗透人员参加的赛事级别和获奖等级而作调整。

## 2.10 鉴定认证

本章包括认证要求、培训学时与鉴定方式、人员要求掌握的知识及法律法规、人员能力要求等内容。

认证要求阐述了各级网络空间安全渗透测试人员的初次申报条件、再认证资格要求、认证省级资格要求。初次申报条件包含学历、从业年限、技术职称要求等等，各个级别的人员认证要求不同，从低级到高级认证要求难度逐级升高，高级别人员要求涵盖低级别人员要求。再认证资格要求规定了人员证书须在有效期内，获证后相关工作从业时间、渗透测试相关领域课程学习时间、通过相关等级的理论和技能考核。认证升级资格要求规定了人员通过认证且证书未失效，人员满足高一级别的认证要求。

各级别人员培训学时从 160 标准学时依次递减，渗透测试一级（初级）人员培训不少于 160 标准学时；渗透测试二级（中级）人员不少于 120 标准学时；渗透测试三级（高级）人员不少于 80 标准学时。考核鉴定包含理论知识及技能实操两部分，理论知识考试时间不少于 90 分钟，技能操作考核时间不少于 120 分钟，综合评审时间不

少于 30 分钟。

网络空间安全渗透测试人员应掌握计算机基础知识、网络安全基础知识、网络安全技术专业知识，熟悉我国关于网络空间安全的相关法律法规。

网络空间安全渗透测试一、二、三级人员的技能要求和相关知识要求依次递进，高级别涵盖低级别的要求。主要包括安全研究、脆弱性测试、渗透测试、修复防护、培训指导等方向。此外，还对知识理论及技能要求的各部分内容作出了权重设置。

### **2.11 解决的问题**

此标准规定了网络空间安全渗透测试人员的人员等级与认证、人员基本要求、直接认证要求、培训鉴定认证要求、考核鉴定权重，对于规范网络空间安全行业渗透测试人员评价认证管理有着积极作用，有利于促进网络空间安全渗透测试人员的培养，为网络空间安全行业发展提供人才资源。

## **三、知识产权情况说明**

本标准不涉及专利。

## **四、采用国际标准和国外先进标准情况**

无。

## **五、与现行相关法律、法规、规章及相关标准的协调性**

建议本标准推荐性实施。本标准不触犯国家现行法律法规，不与其他强制性国标相冲突。

## **六、重大分歧意见的处理经过和依据**

《网络空间安全专业人员能力评价 第1部分：渗透测试》编制过程中未出现重大分歧。

## 七、标准性质的建议

建议《网络空间安全专业人员能力评价 第1部分：渗透测试》作为推荐性团体标准发布实施。

## 八、贯彻标准的要求和措施建议

鉴于本标准是网络安全测试能力人员评价规范，用于评价网络安全相关测试人员的能力，建议在标准贯彻执行过程中，各单位应当起到协调以及推广的作用。

## 九、替代或废止现行相关标准的建议

无替代或废止。

## 十、其他应予说明的事项

无。

《网络空间安全专业人员能力评价 第1部分：渗透测试》

标准编制组

2021年07月