信息安全测试员
国家职业技能标准
（征求意见稿）

1　职业概况

1.1　职业名称

信息安全测试员（信息安全渗透测试员）

1.2　职业编码

4-04-04-04

1.3　职业定义

是指通过对评测目标的网络和系统进行渗透测试，发现安全问题并提出改进建议，使网络和系统免受恶意攻击的人员。

1.4　职业技能等级

本职业共设四个等级，分别为：四级/中级工、三级/高级工、二级/技师、一级/高级技师。

1.5　职业环境条件

室内，常温。

1.6　职业能力特征

具有一定的学习、观察、推理、判断、表达、计算能力；有较强的问题分析、独立工作、沟通交往、协调合作等能力，心理健康。

1.7　普通受教育程度

高中毕业（含）以上（或同等学力）

1.8　培训参考学时

四级/中级工、三级/高级工 不少于 160 标准学时；二级/技师 不少于 120 标准学时；一级/高级技师 不少于 80 标准学时。

1.9　职业技能鉴定要求

1.9.1　申报条件

具备以下条件之一者，可申报四级/中级工：

（1）取得相关职业[1]五级/初级工职业资格证书（技能等级证书）后，累计从事本职业或相关职业工作 2 年（含）以上。

---

[1] 相关职业：网络与信息安全管理员、信息安全工程技术人员、通信工程技术人员、计算机硬件工程技术人员、计算机软件工程技术人员、计算机网络工程技术人员、信息系统分析工程技术人员、信息通信网络运行管理员、信息通信信息化系统管理员、计算机程序设计员、计算机软件测试员等。

（2）累计从事本职业或相关职业工作3年（含）以上。

（3）取得技工学校本专业或相关专业[2]毕业证书（含尚未取得毕业证书的在校应届毕业生）；或取得经评估论证、以中级技能为培养目标的中等及以上职业学校本专业或相关专业[3]_[5]毕业证书（含尚未取得毕业证书的在校应届毕业生）；

具备以下条件之一者，可申报三级/高级工：

（1）取得本职业或相关职业四级/中级工职业资格证书（技能等级证书）后，累计从事本职业或相关职业工作3年（含）以上。

（2）取得本职业或相关职业四级/中级工职业资格证书（技能等级证书），并具有高级技工学校、技师学院毕业证书（含尚未取得毕业证书的在校应届毕业生）；或取得本职业或相关职业四级/中级工职业资格证书（技能等级证书），并具有经评估论证、以高级技能为培养目标的高等职业学校本专业或相关专业[4]毕业证书（含尚未取得毕业证书的在校应届毕业生）。

（3）具有大专及以上本专业或相关专业[5]毕业证书，并取得本职业或相关职业四级/中级工职业资格证书（技能等级证书）后，累计从事本职业或相关职业工作2年（含）以上。

具备以下条件之一者，可申报二级/技师：

（1）取得本职业或相关职业三级/高级工职业资格证书（技能等级证书）后，累计从事本职业或相关职业工作4年（含）以上。

（2）取得本职业或相关职业三级/高级工职业资格证书（技能等级证书）的高级技工学校、技师学院毕业生，累计从事本职业或相关职业工作 3 年（含）以上；或取得本职业或相关职业预备技师证书的技师学院毕业生，累计从事本职业或相关职业工作2年（含）以上。

具备以下条件者，可申报一级/高级技师：

信息安全渗透测试员：

---

[2]相关专业（技工学校）：计算机网络应用、计算机程序设计、计算机应用与维修、计算机信息管理、通信网络应用、通信运营服务、网络安防系统安装与维护、物联网应用技术、网络与信息安全、云计算技术应用、工业互联网技术应用、人工智能技术应用、数字媒体技术应用等信息类专业。

[3]相关专业（中等职业学校）：数字媒体技术应用、计算机平面设计、计算机网络技术、网站建设与管理、网络安防系统安装与维护、软件与信息服务、客户信息服务、计算机与数码产品维修、电子与信息技术、电子技术应用、通信技术、通信运营服务、通信系统工程安装与维护、物联网技术应用、网络信息安全、移动应用技术与服务等信息技术类专业。

[4]相关专业（高等职业学校）：计算机应用技术、计算机网络技术、计算机信息管理、计算机系统与维护、软件技术、软件与信息服务、嵌入式技术与应用、数字展示技术、数字媒体应用技术、信息安全与管理、移动应用开发、云计算技术与应用、大数据技术与应用、人工智能技术服务等计算机类专业。

[5]相关专业（普通高等学校本科）：信息安全、计算机科学与技术、软件工程、网络工程、物联网工程、数字媒体技术、智能科学与技术、空间信息与数字技术、电子与计算机工程、数据科学与大数据技术、网络空间安全、新媒体技术、保密技术、服务科学与工程、虚拟现实技术、区块链工程、网络安全与执法等计算机类、电子信息类专业。

取得本职业或相关职业二级/技师职业资格证书（技能等级证书）后，累计从事本职业或相关职业工作 3 年（含）以上。

1.9.2 鉴定方式

鉴定方式分为理论知识考试、技能考核以及综合审定。理论知识考试笔试、机考等方式为主，主要考核从业人员从事本职业应掌握的基本要求和相关知识要求；技能考核主要采用现场操作、模拟操作等方式进行，主要考核从业人员从事本职业应具备的技能水平；综合审定主要针对技师和高级技师，通常采取审阅申报材料、答辩等方式进行全面评议和审查。

理论知识考试、技能考核和综合审定均实行百分制，成绩皆达 60 分（含）以上者为合格。

1.9.3 监考人员、考评人员与考生配比

理论知识考试中的监考人员与考生配比为 1∶15，且每个考场不少于 2 名监考人员；技能考核中的考评人员与考生配比不低于 1∶5，且考评人员为 3 名（含）以上单数；综合审定委员为 3 人（含）以上单数。

1.9.4 鉴定时间

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，综合审定时间不少于 30 分钟。

1.9.5 鉴定场所设备

理论知识考试在标准教室进行；技能操作考核在具有必备的网络环境、软硬件资源，安全设施完善的场所进行。

2 基本要求

2.1 职业道德

2.1.1 职业道德基本知识

2.1.2 职业守则

（1）遵纪守法，保密合规。

（2）廉洁自律，可靠可信。

（3）牢记职责，爱岗敬业。

（4）客观严谨，公平公正。

（5）流程规范，操作安全。

（6）认真负责，团结协作。

（7）挑战自我，勇于创新。

2.2 基础知识

2.2.1 计算机基础知识

（1） 操作系统知识。

（2） 应用软件知识。

（3） 数据库知识。

（4） 计算机网络知识。

2.2.2 网络安全基础知识

（1）网络安全基本概念。

（2）网络安全模型。

（3）密码学基础知识。

2.2.3 网络安全技术专业知识

（1）WEB 安全专业知识。

（2）网络协议安全专业知识。

（3）中间件安全专业知识。

（4）操作系统安全专业知识。

（5）数据库安全专业知识。

（6）密码学专业知识。

（7）社会工程学专业知识。

（8）安全审计技术专业知识。

（9）反恶意软件与入侵检测技术专业知识。

（10）备份与恢复技术专业知识。

2.2.4 工作常用知识

（1）应用文写作的一般要求。

（2）网络与信息安全专业英语基本词汇。

2.2.5 相关法律、 法规知识

（1）《中华人民共和国民法典》的相关知识。

（2）《中华人民共和国劳动法》的相关知识。

（3）《中华人民共和国劳动合同法》的相关知识。

（4）《中华人民共和国网络安全法》的相关知识。

（5）《中华人民共和国密码法》的相关知识。

（6）《中华人民共和国数据安全法》(草案)的相关知识。

（7）《中华人民共和国个人信息保护法》(草案)的相关知识。

（8）《网络安全审查办法》的相关知识。

（9）《网络安全漏洞管理规定》（待颁布）的相关知识。

（10）《网络安全威胁信息发布管理办法》（待颁布）的相关知识。

（11）网络安全技术标准的相关知识。

（12）其他网络安全相关法律法规、政策、管理规定相关知识。

3 工作要求

本标准对四级/中级工、三级/高级工、二级/技师、一级/高级技师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。

3.1 四级/中级工（信息安全渗透测试员）

职业功能	工作内容	技能要求	相关知识要求
1.安全研究	1.1 漏洞信息研究	1.1.1 能查阅公开的安全漏洞（以下简称漏洞）报告，梳理漏洞分析报告 1.1.2 能收集已公开的漏洞验证程序 1.1.3 能评估测试结果漏洞等级	1.1.1 CNNVD（中国国家信息安全漏洞库）、CNVD（国家信息安全漏洞共享平台）、CVE(Common Vulnerabilities & Exposures)等平台使用方法 1.1.2 漏洞报告梳理方法 1.1.3 CNNVD（中国国家信息安全漏洞库）、CNVD（国家信息安全漏洞共享平台）、CVE(Common Vulnerabilities & Exposures)等平台漏洞原理 1.1.4 已公开漏洞验证程序检索方法 1.1.5 漏洞等级评定方法
	1.2 漏洞工具研究	1.2.1 能检索已披露的漏洞的测试方法、工具 1.2.2 能搭建漏洞测试与测试工具所需的运行环境	1.2.1 漏洞测试环境搭建方法 1.2.2 漏洞触发原理
2.脆弱性测试	2.1 信息收集	2.1.1. 能根据测试对象类型确认测试工具 2.1.2 能根据授权文件确定测试对象边界 2.1.3 能使用信息收集工具完成信息收集工作	2.1.1 域名的基本概念 2.1.2 信息收集工作方法 2.1.3 信息收集工具使用方法
	2.2 测试实施	2.2.1 能配置、使用渗透测试工具完成测试 2.2.2 能确认扫描工作执行的工作状态 2.2.3 能配置、使用压力测试工具完成测试	2.2.1 渗透测试工具配置方法 2.2.2 渗透测试工具使用方法 2.2.3 扫描状态确认方法 2.2.4 压力测试工具配置方法 2.2.5 压力测试工具使用方法
3.渗透测试	3.1 环境恢复	3.1.1 能区分测试过程中所产生的数据类型 3.1.2 能评估测试所产生数据对信息系统的影响	3.1.1 系统、应用日志等常见数据类型 3.1.2 应用系统功能、业务流程 3.1.3 渗透测试操作影响评估方法
	3.2 测试管理	3.2.1 能根据测试工作流程确定使用测试工具类型 3.2.2 能根据标准测试项选择测试方案	3.2.1 渗透测试工具确认方法 3.2.2 测试方案选择方法

4.修复防护	4.1 测试报告编制	4.1.1.能根据模板整理测试获得的数据 4.1.2 能根据测试报告模板整理相关的测试记录	4.1.1 测试数据归档方法 4.1.2 测试记录整理方法
	4.2 漏洞修复测试	4.2.1 能根据测试工具输出的测试报告验证漏洞 4.2.2 能借助漏洞测试工具验证漏洞修复效果	4.2.1 漏洞测试工具使用方法 4.2.2 漏洞验证方法 4.2.3 漏洞复测方法

3.2 三级/高级工（信息安全渗透测试员）

职业功能	工作内容	技能要求	相关知识要求
1.安全研究	1.1 漏洞信息研究	1.1.1 能收集已公开高危漏洞信息进行漏洞研究，编写漏洞复现报告 1.1.2 能评估已公开漏洞的危害、影响范围，提交漏洞评估报告	1.1.1 CNNVD（中国国家信息安全漏洞库）、CNVD（国家信息安全漏洞共享平台）、CVE(Common Vulnerabilities & Exposures)等平台漏洞库体系知识 1.1.2 漏洞复现报告编写方法 1.1.3 公开漏洞危害评估方法 1.1.4 漏洞评估报告编写方法
	1.2 漏洞工具研究	1.2.1 能验证已披露漏洞测试工具的有效性 1.2.2 能根据已有的漏洞代码片段编写漏洞触发代码	1.2.1 已披露漏洞的测试工具使用方法 1.2.2 漏洞触发代码编写方法
2.脆弱性测试	2.1 信息收集	2.1.1 能使用自动化和人工相结合完成信息收集工作 2.1.2 能梳理、分析信息收集结果	2.1.1 人工信息收集方法 2.1.2 多维度数据关联分析方法
	2.2 测试实施	2.2.1 能通过资产风险寻找测试突破口 2.2.2 能根据给定测试项人工实施漏洞测试工作 2.2.3 能根据目标系统实际情况制定压力测试策略，确定测试指标	2.2.1 渗透测试实施流程 2.2.2 漏洞验证方法 2.2.3 人工渗透方法 2.2.4 压力测试实施方法
3.渗透测试	3.1 测试准备	3.1.1 能判断业务高峰期，错峰进行渗透测试 3.1.2 能评估所使用测试手段对系统的业务影响	3.1.1 系统业务负载判断方法 3.1.2 漏洞原理及影响
	3.2 环境恢复	3.2.1 能确定环境恢复的内容 3.2.2 能对环境恢复提出建议	3.2.1 数据文件查找方法 3.2.2 日志文件分析方法
	3.3 测试管理	3.3.1 能根据测试对象确定测试流程 3.3.2 能根据日志文件判断对应的行为 3.3.3 能根据测试工作实施过程中的异常情况，发现不规范的操作或失误	3.3.1 渗透测试实施方法 3.3.2 测试异常情况判断方法 3.3.3 测试异常应急处置方法

4.修复防护	4.1 测试报告编制	4.1.1 能梳理测试过程中获取的数据 4.1.2 能根据测试结果编写测试报告	4.1.1 测试数据处理方法 4.1.2 测试报告编制方法
	4.2 漏洞修复测试	4.2.1 能根据测试项及测试结果，给出修复建议 4.2.2 能根据测试报告，验证漏洞修复效果	4.2.1 人工漏洞验证方法 4.2.2 漏洞验证工具使用方法 4.2.3 漏洞修复方法

3.3 二级/技师（信息安全渗透测试员）

职业功能	工作内容	技能要求	相关知识要求
1.安全研究	1.1 漏洞信息研究	1.1.1 能根据已公开的高危漏洞信息，编写漏洞利用流程报告 1.1.2 能根据官方发布的漏洞信息提出解决方法	1.1.1 漏洞攻击原理，漏洞防护、绕过原理 1.1.2 漏洞利用流程报告编写方法
	1.2 漏洞工具研究	1.2.1 能优化已公开漏洞测试工具 1.2.2 能集成开发漏洞验证程序用于测试工作	1.2.1 漏洞测试工具原理 1.2.2 漏洞验证程序集成开发方法
	1.3 漏洞发现	1.3.1 能在有目标系统源码的基础上进行漏洞挖掘 1.3.2 能使用代码审计的方式测试目标漏洞	1.3.1 常见(例如收录于 CNVD 中的漏洞）应用漏洞挖掘方法 1.3.2 代码审计方法
2.漏洞测试	2.1 信息收集	2.1.1 能使用人工方式收集信息 2.1.2 能使用社会工程学并结合技术手段获取测试目标信息 2.1.3 能根据测试对象的业务逻辑绘制业务数据流向图	2.1.1 社交工具、搜索引擎使用方法 2.1.2 社会工程学概念及实施方法 2.1.3 业务逻辑流程，业务数据流绘图方法
	2.2 测试实施	2.2.1 能根据误报信息优化测试工具的使用策略 2.2.2 能根据业务逻辑，测试业务逻辑漏洞 2.2.3 能编写压力测试脚本，并对目标进行压力测试 2.2.4 能对压力测试数据进行分析，编写压力测试报告	2.2.1 测试工具使用策略优化方法 2.2.2 系统调用逻辑、业务逻辑交互方式 2.2.3 业务逻辑漏洞测试思路 2.2.4 压力测试脚本编写方法 2.2.5 压力测试数据分析方法 2.2.6 压力测试报告编写方法
3.渗透测试	3.1 漏洞利用	3.1.1 能利用多漏洞联合方式进行测试 3.1.2 能完整记录漏洞利用过程 3.1.3 能绕过安全防御机制进行测试 3.1.4 能制定测试路径 3.1.5 能进行社会工程学测试进行测试工作	3.1.1 漏洞关联分析方法 3.1.2 漏洞利用过程记录方法 3.1.3 安全设备检测机制原理 3.1.4 安全防御机制绕过方法 3.1.5 测试路径分析方法 3.1.6 社会工程学实施方法

	3.2 环境恢复	3.2.1 能确认测试对象相关的数据及资料完整和准确 3.2.2 能确认环境恢复	3.2.1 测试数据确认要求 3.2.2 环境恢复要求 3.2.2 环境恢复确认方法
	3.3 测试管理	3.3.1 能实施测试工作中的风险规避措施及应急预案 3.3.2 能在实施过程中进行风险管控 3.3.3 能编写用于指导测试实施工作的安全测试计划 3.3.4 能编写用于指导测试实施工作的安全测试技术指南	3.3.1 测试操作异常识别方法 3.3.2 测试异常情况处理流程 3.3.3 信息系统风险管控要求 3.3.4 测试实施计划编写方法 3.3.5 测试技术指南编写方法
4．修复防护	4.1 测试报告编制	4.1.1 能讲解测试过程 4.1.2 能编写测试报告模板	4.1.1 测试过程要点 4.1.2 测试报告模板编写方法
	4.2 漏洞修复建议	4.2.1 能给出通用型漏洞修复建议 4.2.2 能给出业务逻辑漏洞的修复建议	4.2.1 通用型漏洞修复原理 4.2.2 业务逻辑漏洞原理、修复方法
5.培训指导	5.1 培训实施	5.1.1 能制订培训工作计划 5.1.2 能编制和实施培训方案 5.1.3 能编写本职业培训教材、讲义、课件 5.1.4 能进行本职业培训宣讲	5.1.1 本职业技能与理论基础知识 5.1.2 培训工作计划的制订要求和方法 5.1.3 培训方案编制和实施的要求和方法 5.1.4 培训教材、讲义、课件的编写知识 5.1.5 教学教法知识
	5.2 技术指导	5.2.1 能对本职业三级/高级工及以下级别人员进行技能指导 5.2.2 能对本职业三级/高级工及以下级别人员技能水平进行考核	5.2.1 操作经验和技能总结方法 5.2.2 技能和理论基础知识水平考核的要求和方法 5.2.3 技能和理论基础知识水平考核的内容

3.4　一级/高级技师（信息安全渗透测试员）

职业功能	工作内容	技能要求	相关知识要求
1.安全研究	1.1 漏洞信息研究	1.1.1 能研究漏洞影响范围，编写漏洞预警报告 1.1.2 能判断漏洞的补丁或临时解决方案对漏洞防范的有效性	1.1.1 漏洞防护方法 1.1.2 漏洞预告报告编写方法
	1.2 漏洞工具研究	1.2.1 能分析漏洞信息并编写漏洞触发代码 1.2.2 根据漏洞触发代码，编写漏洞测试工具	1.2.1 漏洞信息分析方法 1.2.2 漏洞检测工具编写方法

	1.3 漏洞发现	1.3.1 能发现未知漏洞。 1.3.2 能对发现的未知漏洞进行评估，编写漏洞说明材料。	1.3.1 漏洞原理分析方法 1.3.2 漏洞说明文件编写方法
2.漏洞测试	2.1 信息收集	2.1.1 能编写信息收集工具 2.1.2 能更新迭代信息收集工具	2.1.1 信息收集工具编写方法 2.1.2 信息收集工具迭代方法
	2.2 测试实施	2.2.1 能结合测试场景制定测试工具的使用策略 2.2.2 能编写测试工具 2.2.3 能根据压力测试结果，给出针对性的系统优化方案	2.2.1 代码审计原理 2.2.2 测试工具编写方法 2.2.3 测试报告审定方法 2.2.4 系统性能优化方法
3.渗透测试	3.1 隐患处置	3.1.1 能发现系统内隐藏的恶意程序 3.1.2 能对系统内隐藏的恶意程序进行分析、处置或溯源	3.1.1 恶意程序发现方法 3.1.2 恶意程序分析处置方法 3.1.2 恶意程序溯源方法
	3.2 测试管理	3.2.1 能评估信息系统异常情况类型和级别等指标 3.2.2 能制定测试工作应急预案，解决异常问题 3.2.3 能审定、优化安全测试技术指南 3.2.4 能审定、优化实施计划	3.2.1 测试异常情况区分标准 3.2.2 测试突发情况处理方法 3.2.3 安全事件影响等级的评估方法 3.2.4 应急预案编制方法 3.2.5 安全测试方法、原理 3.2.6 技术指南、实施计划审定方法
4．修复防护	4.1 测试报告编制	4.1.1 能审定、优化测试报告 4.1.2 能审定、优化测试报告模板	4.1.1 测试报告审定、优化方法 4.1.2 测试报告模板审定、优化方法
	4.2 漏洞修复建议	4.2.1 能对测试对象给出具体修复建议 4.2.2 能对整体信息系统给出安全优化建议	4.2.1 安全防护、安全检测标准 4.2.2 系统整体架构 4.2.3 系统整体安全优化方法
5.培训指导	5.1 培训实施	4.1.1 能对培训需求进行分析 4.1.2 能编制培训规划 4.1.3 能组织编写本职业培训教材、讲义、教案 4.1.4 能进行本职业培训宣讲	4.1.1 培训需求分析的要求和方法 4.1.2 培训规划编制的要求 4.1.3 培训预算与决算的审核方法
	5.2 技术指导	4.2.1 能对本职业各级别人员技能进行指导 4.2.2 能对本职业各级别人员技能水平进行考核 4.2.3 能组织开展技术革新活动	4.2.1 操作技能方法 4.2.2 指导技能操作的知识 4.2.3 技术革新的方法

4　权重表

4.1 理论知识权重表

4.1.1 理论知识权重表（信息安全渗透测试员）

技能等级 项目		四级/ 中级工 （%）	三级/ 高级工 （%）	二级/ 技师 （%）	一级/ 高级技师 （%）
基本 要求	职业道德	5	5	5	5
	基础知识	20	10	5	5
相关 知识 要求	安全研究	25	20	20	25
	脆弱性测试	25	30	25	25
	渗透测试	20	30	25	20
	修复防护	5	5	10	10
	培训指导			10	10
合计		100	100	100	100

4.2 技能要求权重表

4.2.1 技能要求权重表（信息安全渗透测试员）

技能等级 项目		四级/ 中级工 （%）	三级/ 高级工 （%）	二级/ 技师 （%）	一级/ 高级技师 （%）
技能 要求	安全研究	30	30	25	30
	脆弱性测试	30	30	25	25
	渗透测试	20	30	25	20
	修复防护	20	10	10	10
	培训指导			15	15
合计		100	100	100	100