ICS xxxxxx
P xxx

团　　体　　标　　准

T/GDCSA XXX—2021

网络空间安全专业人员能力评价
第 1 部分：渗透测试

Competence Evaluation of Cyberspace Security Professionals

Part 1: Penetration Testing

（征求意见稿）

2021－ ××－ ××发布　　2021－ ××－ ××实施

广东省网络空间安全协会发布

目　次

前　言

本文件按照 GB/T 1.1—2020给出的规则起草。
本文件由网安联认证服务有限公司提出。
本文件由广东省网络空间安全协会归口。
本文件起草单位：。
本文件主要起草人：。
本文件为首次修订。

网络空间安全专业人员能力评价 第1部分：渗透测试

1 范围

本文件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、考核鉴定权重等。

本文件适用于对渗透测试人员进行培训和认证。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用千本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

渗透测试 Penetration test

通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全的一种评估方法。

3.2

渗透测试人员 Penetration testing professionals

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。

4 认证级别

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。该类人员应具有较好的学习、观察、分析、推理、判断、表达、计算、独

立工作、沟通交往、协调合作等能力且心理健康。

5 认证方式

5.1 直接认证

在地级以上市举办的网络安全攻防与应急实战演练、CTF类竞赛、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，该人员可选择性参与技能培训。

5.2 鉴定认证

人员通过专业技能培训，经考核鉴定后方可颁发相应的等级认证证书，证书有效期为3年。

鉴定认证方式分为理论知识考试、技能考核以及综合评审。理论知识考试以笔试、机考等方式为主，主要考核渗透测试人员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，主要考核渗透测试人员应具备的技能水平；综合评审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、技能考核和综合评审均实行百分制，成绩皆达 60 分（含）以上者为合格，可获得认证证书。

6 人员基本要求

获证人员应满足如下基本要求：

（1）具有独立的民事行为能力，具备承担法律责任的能力；

（2）无违法犯罪记录；

（3）不存在法律法规禁止从业的情形；

（4）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；

（5）符合有关法律法规的规定。

7 直接认证

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。认证等级见表1。

表 1　认证等级

参赛获奖记录	认证等级
在省市级竞赛或演练中获得三等奖或等同于三等奖的奖项或荣誉；	渗透测试一级（初级）人员
在省市级竞赛或演练中获得二等奖或等同于二等奖的奖项或荣誉； 在国家级或行业竞赛或演练中获得三等奖或等同于三等奖的奖项或荣誉；	渗透测试二级（中级）人员
在省市级竞赛或演练中获得一等奖或等同于一等奖的奖项或荣誉； 在国家级或行业竞赛或演练中获得二等奖或等同于二等奖及以上的奖项或荣誉；	渗透测试三级（高级）人员

8　鉴定认证

8.1 认证要求

8.1.1 初次申报条件

8.1.1.1 具备以下条件之一者，经过培训，通过考试者，可申报渗透测试一级（初级）人员：

（1）本科（含）以上学历，从事本职业或相关职业工作；

（2）大专以上学历，2年（含）以上从事本职业或相关职业工作经历；

（3）累计从事本职业或相关职业工作4年（含）以上；

（4）具有网络空间安全相关专业的初级（含）以上技术职称。

8.1.1.2 具备以下条件之一者，经过培训，通过考试者，可申报渗透测试二级（中级）人员：

（1）取得本职业或相关职业渗透测试一级（初级）人员证书后，累计从事本职业或相关职业工作 2年（含）以上。

（2）硕士研究生（含）以上学历，从事本职业或相关职业工作；

（3）本科毕业，2年以上从事本职业或相关职业工作经历；

（4）专科毕业，4年以上从事本职业或相关职业工作经历；

（5）累计从事本职业或相关职业工作6年（含）以上；

（6）具有网络空间安全相关专业的中级（含）以上技术职称。

8.1.1.3 具备以下条件之一者，经过培训，通过考试者，可申报渗透测试三级（高级）人员：

（1）取得本职业或相关职业渗透测试二级（中级）人员证书后，累计从事本职业或相关职业工作 2年（含）以上。

（2）硕士研究生（含）以上学历， 2年以上从事本职业或相关职业工作经历；

（3）本科毕业，4年以上从事本职业或相关职业工作经历；

（4）专科毕业，6年以上从事信息安全有关工作经历，并且至少3年以上从事与申请认证专业方向相关的工作经历；

（5）8年以上从事本职业或相关职业工作经历；

（6）具有网络空间安全相关专业的高级技术职称。

8.1.2 再认证资格要求

（1）已通过渗透测试人员等级认证，且在认证有效期内；

（2）获证后 2 年内至少有 1 年的工作或学习经历与获得认证的专业方向相关；

（3）每年不少于 16 小时的渗透测试相关领域的持续发展课程学习。

（4）必须通过相关等级的理论知识和技能考核。

8.1.3 认证升级资格要求

（1）已通过渗透测试人员认证，且在认证有效期内；

（2）满足渗透测试人员认证高一级别认证要求，包括工作或学习经历、培训和考试要求。

8.2 培训学时与鉴定方式

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。

8.3 人员知识及法律法规要求

8.3.1 计算机基础知识

（1）操作系统知识

a. 计算机硬件基础知识

b. 计算机软件基础知识

c. 操作系统基础知识

（2）办公应用软件知识

（3）防病毒知识

a. 计算机恶意程序识别知识

b. 计算机恶意程序查杀

（4）数据库知识

（5）计算机网络知识

a. 网络协议基础知识

b. 组网基础知识

c. 网络配置、查排障常用命令和工具使用

8.3.2 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）网络安全管理和技术概述

（4）新技术新应用安全概述

（5）访问控制理论基础知识

（6）博弈论基础知识

（7）近代密码心理学知识

8.3.3 网络安全技术专业知识

（1）网络安全专业知识

（2）WEB 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）密码编码学与破译学专业知识

（7）社会工程学专业知识

（8）安全审计技术专业知识

（9）入侵检测技术专业知识

（10）备份与恢复技术专业知识

8.3.4 熟悉相关法律法规

（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）《网络安全等级保护条例（征求意见稿）》的相关知识

（7）《关键信息基础设施安全保护条例（征求意见稿）》的相关知识

（8）《网络安全审查办法(征求意见稿)》的相关知识

（9）《网络安全漏洞管理规定(征求意见稿)》的相关知识

（10）《网络安全威胁信息发布管理办法(征求意见稿)》的相关知识

（11）《信息安全等级保护管理办法》（公通字43号)的相关知识

（12）《工业互联网企业网络安全分类分级指南(试行)》(征求意见稿)的相关知识

（13）《信息安全技术网络安全等级保护基本要求》、《信息安全技术网络安全等级保护测评要求》、《信息安全技术网络安全等级保护安全设计技术要求》三项国家标准的相关知识

（14）其他网络安全相关法律法规、政策、管理规定和标准的相关知识

8.4 人员工作能力要求

本标准对一、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。

8.4.1 渗透测试一级（初级）人员

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、CVE 等主流漏洞平台使用方法 1.1.2 漏洞报告梳理方法 1.1.3 CVE、CNNVD 平台常见漏洞原理 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 漏洞测试工具环境搭建方法 1.2.2 常用漏洞代码原理 1.2.3 漏洞触发代码编写方法

职业功能	工作内容	技能要求	相关知识要求
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 能够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 信息收集工具使用方法 2.1.3 信息收集工作方法
	2.2 脆弱性测试	2.2.1 能使用、配置脆弱性测试工具完成测试 2.2.2 能确认扫描工作执行的工作状态 2.2.3 能使用、配置压力测试工具完成压力测试	2.2.1 脆弱性测试工具使用方法 2.2.2 脆弱性测试工具配置方法 2.2.3 脆弱性扫描状态确认方法 2.2.4 压力测试工具使用方法 2.2.5 压力测试工具配置方法
3.渗透测试	3.1 清除数据	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 常见应用系统功能、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 能根据标准测试项确定测试方向	3.2.1 渗透测试工具确认方法 3.2.2 常见渗透测试工具使用方法 3.2.3 测试方向规划方法
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 能根据脆弱性测试工具输出的测试报告验证漏洞准确性 4.2.2 能借助脆弱性测试工具验证漏洞修复效果	4.2.1 常见脆弱性原理相关知识 4.2.2 脆弱性测试工具使用方法 4.2.3 脆弱性验证方法 4.2.4 漏洞复测方法

8.4.2 渗透测试二级（中级）人员

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 能够跟踪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 历史高危漏洞的演进过程 1.1.2 官方公布的漏洞修复原理 1.1.3 漏洞攻击原理，漏洞防护、绕过原理 1.1.4 漏洞利用流程报告编写方法

职业功能	工作内容	技能要求	相关知识要求
	1.2 漏洞工具研究	1.2.1 能够优化已公开漏洞测试工具 1.2.2 能够集成漏洞验证程序用于测试工作	1.2.1 脚本编写方法 1.2.2 漏洞测试工具原理知识 1.2.3 漏洞验证程序集成开发方法
	1.3 漏洞发现	1.3.1 能挖掘常见(例如收录于CNVD中的可复现漏洞）应用漏洞 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中的可复现漏洞）应用漏洞挖掘方法 1.3.2 代码审计方法
2.脆弱性测试	2.1 信息收集	2.1.1能使用手工方式收集信息 2.1.2 能使用社会工程学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 多维度数据关联分析方法 2.1.4 常见业务逻辑流程 2.1.5 业务数据流绘图方法
	2.2 脆弱性测试	2.2.1 能够根据误报信息优化脆弱性测试工具的策略 2.2.2 能够根据业务逻辑，测试业务逻辑脆弱性 2.2.3 能编写压力测试脚本，对压力测试数据进行分析，编写压力测试报告	2.2.1 脆弱性测试工具原理 2.2.2 脆弱性测试工具策略优化方法，比如打虚拟补丁等 2.2.3 常见业务流程、系统调用逻辑、业务逻辑交互方式 2.2.4 常见业务逻辑脆弱性测试思路 2.2.5 压力测试脚本编写方法 2.2.6 压力测试数据分析方法 2.2.7 压力测试报告编写方法
3.渗透测试	3.1 漏洞利用	3.1.1 能根据测试环境，调整提高测试工具效率的配置参数 3.1.2 能利用多漏洞联合方式进行测试 3.1.3 能完整记录漏洞利用过程	3.1.1 系统应用操作方法 3.1.2 相关漏洞原理、漏洞间关联 3.1.3 漏洞利用过程记录方法
	3.2 清除数据	3.2.1能销毁测试期间收集到的与测试对象相关的数据及资料 3.2.2能够验证数据销毁结果，确认数据清除	3.2.1 测试操作注意事项 3.2.2 测试数据及资料清理方法 3.2.3 数据销毁校验方法
	3.3 测试管理	3.3.1 能执行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，协助测试对象单位完成应急响应工作 3.3.3 能编写用于指导测试实	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 信息系统风险管控知识 3.3.4 测试技术指南 3.3.5 测试实施计划编写方法

职业功能	工作内容	技能要求	相关知识要求
		施工作的安全测试实施计划 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	
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 本职业技能与理论基础知识 4.1.2 测试报告模板编写方法
	4.2 漏洞修复建议	4.2.1 能根据通用防护手段给出一般性漏洞修复建议 4.2.2 能对业务逻辑漏洞给出针对性漏洞修复建议	4.2.1 漏洞防护知识 4.2.2 常见业务逻辑漏洞原理、修复方法
5.培训指导	5.1 测试技能培训	5.1.1 能开展安全意识培训 5.1.2 能为四级、三级信息安全测试员进行测试技能培训	5.1.1 信息系统攻防基础知识 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 教学教法知识
	5.2 测试技能输出	5.2.1 能编写测试检查项 5.2.2 能根据网络环境及业务模式制定特有的测试方案 5.2.3 能根据行业实际情况编写面向信息安全测试员从业者培训教材	5.2.1 测试检查项编写方法 5.2.2 常见业务模式 5.2.3 渗透测试方案编写方法 5.2.4 教材编写方法 5.2.5 操作经验和技能总结方法

8.4.3 渗透测试三级（高级）人员

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，提交漏洞预警报告 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 常见漏洞原理及防护方法 1.1.2 漏洞影响范围分析知识 漏洞预警报告编写方法
	1.2 漏洞工具研究	1.2.1 能根据漏洞触发代码编写漏洞测试工具 1.2.2 能根据漏洞预警信息，发掘漏洞相关信息，编写漏洞测试工具	1.2.1 已公开漏洞触发代码的原理及程序编码方法。（说明：根据已经公开的 poc 、exp 编写批量扫描工具，可以集成到脆弱性工具，或者单独使用，给初级人员使用，这里的工具更多针对平时的漏洞挖掘研究使用。） 1.2.2 未公开细节漏洞检测工具编写方法 1.2.3 漏洞测试作经验总结方法
	1.3 漏洞发现	1.3.1 能对已经未完全公开的漏洞详情进行分析，完成漏洞评估，编写漏洞说明材料 1.3.2 能够挖掘利用成本低、影响程度深、修复难度大的超危漏洞	1.3.1 漏洞原理分析方法 1.3.2 漏洞说明文件编写方法 1.3.3 超危漏洞挖掘方法
2.脆弱性测试	2.1 信息收集	2.1.1 能根据收集的信息特征，编写信息收集工具 2.1.2 能更新迭代编写的信息收集工具	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 脆弱性测试	2.2.1 能结合测试场景自定义脆弱性测试工具的策略 2.2.2 能编写脆弱性测试工具 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 常见场景下测试策略 2.2.2 代码审计原理 2.2.3 脆弱性测试工具使用方法 2.2.4 脆弱性测试工具编写方法 2.2.5 脆弱性报告评审方法 2.2.6 系统性能优化方法
3.渗透测试	3.1 漏洞利用	3.1.1 能绕过安全防御机制进行测试工作 3.1.2 能制定攻击路径进行测试工作 3.1.3 能进行社会工程学攻击进行测试工作	3.1.1 安全设备检测机制原理 3.1.2 安全防御机制绕过方法 3.1.3 测试路径分析方法 3.1.4 社会工程学攻击方法

职业功能	工作内容	技能要求	相关知识要求
	3.2 清除数据	3.2.1 能执行反溯源工作 3.2.2 能对系统内隐藏的恶意程序进行指导清除工作	3.2.1 路径溯源分析方法 3.2.2 反溯源相关知识 3.2.3 测试数据、程序清除方法 3.2.4 防病毒工具基本原理
	3.3 测试管理	3.3.1 能评估信息系统异常情况类型和级别等指标 3.3.2 能制定测试工作应急预案，解决异常问题 3.3.3 能评审、优化安全测试技术指南 3.3.4 能评审、优化实施计划	3.3.1 测试异常情况区分方法 3.3.2 测试突发情况处理方法 3.3.3 安全事件影响等级的评估方法 3.3.4 应急预案编制方法 3.3.5 安全测试方法、原理 3.3.6 技术指南、实施计划评审方法
4.修复防护	4.1 测试报告编制	4.1.1 能评审、优化测试报告 4.1.2 能编写、优化测试报告模板	4.1.1 测试报告评审、优化方法 4.1.2 测试报告模板编写方法
	4.2 漏洞修复建议	4.2.1 能给出测试对象的具体修复建议 4.2.2 能给出整体信息系统的安全优化建议	4.2.1 安全防护、安全检测原理 4.2.2 系统整体架构知识 4.2.3 系统整体安全优化方法
5.培训指导	5.1 测试技能培训	5.1.1 能对二、三、四级人员及安全团队开展安全趋势评估培训 5.1.2 能开展信息系统安全开发培训 5.1.3 能评估安全设备的优缺点及对比差距	5.1.1 安全知识培训方法 5.1.2 安全开发相关知识 5.1.3 安全设备相关知识 5.1.4 差距评估方法
	5.2 测试技能指导	5.2.1 能评审、优化测试检查项 5.2.2 能评审、优化现有的渗透测试方案 5.2.3 能评审、优化面向信息安全测试员从业者培训教材	5.2.1 本职业技能与理论基础知识 5.2.2 测试检查项审查方法 5.2.3 渗透测试方案审查方法 5.2.4 培训教材审查方法

8.5 考核鉴定权重表

8.5.1 理论知识权重表

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

8.5.2 技能要求权重表

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