ICS 35.020
L 70

团　　体　　标　　准

T/GDCSA 006—2021

网络安全测试能力（团队）评价规范

Specification for the ability evaluation of cyber security testing teams

2021－08－30 发布　　2021－08－31 实施

北京网络空间安全协会
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《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由网安联认证服务有限公司提出。

本文件由北京网络空间安全协会、广东省网络空间安全协会归口。

本文件起草单位：广东关键信息基础设施保护中心、广东新兴国家网络安全和信息化发展研究院、广州华南信息安全测评中心、网安联信息技术有限公司、网安联认证服务有限公司。

本文件主要起草人：邢静、缪静、张伟、黄珊珊。

本文件为首次发布。

网络安全测试能力（团队）评价规范

1 范围

本文件规定了网络安全测试团队能力的评价原则、团队管理、评价指标、评价方法及年审等要求。

本文件适用于第三方机构对网络安全攻防测试团队进行能力评价，可作为网络安全攻防测试服务需求方选择团队的参考依据，也可为网络安全攻防测试团队提高自身水平提供指导。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

网络安全测试团队 cyber security testing team

由主要从事网络安全攻防测试人员以攻防形式组成的团队。

3.2

竞赛 competition

网络安全领域相关的竞赛，包括夺旗模式比赛、攻防模式比赛等。

3.3

攻防演练 offensive and defensive drills

基于预设的网络信息系统保护目标，以网络安全攻击和网络安全防守为主要手段，采用攻防双方对抗方式组织的网络安全演习和训练活动。

3.4

夺旗模式比赛 capture the flag

以在线环境交互或文件离线分析方式进行网络安全技术挑战，提交答案（flag），获取相应分值。

3.5

攻防模式比赛 attack and defense mode competition

以互相攻击和防守方式进行网络安全技术挑战，挖掘网络服务漏洞并攻击对手服务来得分，修补自身服务漏洞进行防御来避免丢分。

3.6

靶场演练 range drills

在真实网络模拟仿真的环境中，对于多层次、多任务的场景进行网络安全挑战，完成既定目标任务。

4 评价原则

4.1 自愿原则

在团队成员自愿的基础上开展能力评价工作。

4.2 公开原则

团队的能力评价规则公开透明。

4.3 公平原则

采用统一、中立、持平的评价规则，以保证评价的公平性。

4.4 公正原则

评价的过程及其结果不受任何方的影响。

5 团队管理

5.1 基本要求

a) 应拥护中国共产党的领导，拥护中国特色社会主义制度；
b) 应具有中华人民共和国国籍，长期在境内居住，无境外永久居留权；
c) 应遵守相关法律法规的规定，无犯罪记录。

5.2 团队构成

团队成员一般由 3-6 人构成，可由 WEB 安全、二进制、逆向、漏洞应用、移动安全等技术方向人员组成。

6 评价指标

6.1 基本要求

必须满足 5.1 要求。

6.2 管理制度要求

团队应具备人员管理、技能培训、风险防范等方面的制度，须接受网络安全行业主管部门的监管，遵纪守法，行为合规，不得违背社会公序良俗。

6.3 能力要求

团队成员获得的网络安全相关认证证书、能力证书、荣誉证书等。

6.4 实战经验

团队应有相关实战比赛经验，如实战演练、CTF 类竞赛、职业技能竞赛等。

6.5 业绩奖项

过去 2 年内，团队在相关比赛中获得的荣誉奖项。

7 评价方法

7.1 指标与赋分

团队评价指标总赋分为 100 分。各项评价内容赋分分别为：基本要求评价 10 分，管理制度要求评价 15 分，能力要求评价 20 分，实战经验评价 20 分，业绩奖项评价 35 分。

网络安全测试团队能力评价指标见附录 A。

7.2 分数计算

总体评价分计算方法见式（1）：

$$S=A+B+C+D+E \cdots\cdots (1)$$

式中：

S ——总体评价分；

A ——基本要求评价；

B ——管理制度要求评价；

C ——能力要求评价；

D ——实战经验评价；

E ——业绩奖项评价。

7.3 等级标准

网络安全测试团队能力评价等级分为一星级、二星级、三星级、四星级、五星级。一星级级别最低，五星级级别最高。评价等级如表 1 所示。

表 1 评价等级

等级	一星级	二星级	三星级	四星级	五星级
评分(分)	45≤S＜55	55≤S＜65	65≤S＜75	75≤S＜90	90≤S

8 年审

每年应进行年审以确保团队符合等级要求，可根据标准要求进行等级调整。

9 其他要求

9.1 满足相应认证级别的要求团队，经申请均可进行认证等级的升级，最高等级为五星级。

9.2 认证有效期满后可进行重新等级评价。

附 录 A
（规范性）
网络安全测试团队能力评价指标

表A 规定了网络安全测试团队能力评价指标。

表A 网络安全测试团队能力评价指标

评价项目	分值	评价内容	评价指标及赋分
基本要求评价	10 分	拥护中国共产党的领导及中国特色社会主义制度	2.5 分
		具有中华人民共和国国籍，长期在境内居住，无境外永久居留权	2.5 分
		无犯罪记录	2.5 分
		遵守相关法律法规的规定	2.5 分
管理制度要求评价	15 分	团队管理制度	2.5 分
		专业的技能培训制度	2.5 分
		有合作训练及安全教育记录	1 次 3 分 2~3 次 5 分 4~10 次 8 分 10 次以上 10 分
能力要求评价	20 分	获得国家级或省级网络安全相关认证证书、能力证书、荣誉证书（厅局级及以上政府部门发放的网络安全相关的嘉奖证书）等	1 人获证 3 分 2 人获证 5 分 3 人及以上获证 10 分

<table>
<tr><th>评价项目</th><th>分值</th><th colspan="2">评价内容</th><th>评价指标及赋分</th></tr>
<tr><td></td><td></td><td colspan="2">不同获证人员的证书类别方向</td><td>1 种类别 3 分
2 种类别 5 分
3 种类别 8 分
4 种以上类别 10 分</td></tr>
<tr><td rowspan="2">实战经验评价</td><td rowspan="2">20 分（超过 20 分以 20 分计）</td><td rowspan="2">过去 2 年内团队成员参加过实战演练,CTF 类竞赛，职业技能竞赛，其它重大创新竞赛或演练等</td><td>竞赛或演练级别[1]（如有决赛，则按进入决赛计）</td><td>A 类赛 10 分/次
B 类赛 8 分/次
C 类赛 5 分/次</td></tr>
<tr><td>参加赛事频次
（如有决赛，则按进入决赛且得分计）</td><td>1 次 5 分
2~5 次 8 分
5 次以上 10 分</td></tr>
<tr><td rowspan="4">业绩奖项评价</td><td rowspan="4">35 分（超过 35 分以 35 分计）</td><td colspan="2">演练类获得一等奖或
等同于相关级别的奖项或荣誉[2]</td><td>A 类赛 30 分/次
B 类赛 25 分/次
C 类赛 20 分/次</td></tr>
<tr><td colspan="2">演练类获得二等奖或
竞赛类获得一等奖或
等同于相关级别的奖项或荣誉；</td><td>A 类赛 25 分/次
B 类赛 20 分/次
C 类赛 15 分/次</td></tr>
<tr><td colspan="2">演练类获得三等奖或
竞赛类获得二等奖或
等同于相关级别的奖项或荣誉；</td><td>A 类赛 20 分/次
B 类赛 15 分/次
C 类赛 10 分/次</td></tr>
<tr><td colspan="2">竞赛类获得三等奖或
等同于相关级别的奖项或荣誉；</td><td>A 类赛 15 分/次
B 类赛 10 分/次
C 类赛 5 分/次</td></tr>
<tr><td colspan="5">注：
[1] 竞赛或演练级别指：
A 类赛：赛事主办方或指导单位级别为国家级及以上，或赛事规模为 5000 人以上；
B 类赛：赛事主办方或指导单位级别为省级或行业级，或赛事规模为 2001~5000 人；
C 类赛：赛事主办方或指导单位级别为市级（统指地级以上市），或赛事规模为 2000 人及以下。
[2] 等同于相关级别的奖项或荣誉指：
在得分选手中，前 1%（不足 1 名按 1 名算）按一等奖算，最多 3 名。1%~3%按二等奖算，最多 6 名，3%~6%按三等奖算，最多 15 名。</td></tr>
</table>