ICS xxxxxx
P xxx

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

（征求意见稿）

2021－ ××－ ××发布　　2021－ ××－ ××实施

广东省网络空间安全协会
广东省计算机信息网络安全协会　发布

目　次

前　言

本文件按照GB/T 1.1—2020给出的规则起草。

本文件由广东省计算机信息网络安全协会提出。

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定原则、团队人员组成、团队的分级、评价指标、团队的认证等要求。

本文件适用于认证机构对网络安全攻防测试团队进行认证，可作为网络安全攻防测试服务需方选择团队的评估依据，另外，也可为网络安全攻防测试团队提高自身能力提供指导。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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

网络安全攻防团队 cyber security attack and defense team

由主要从事网络安全攻防测试人员以攻方和防守方的形式组成的团队。

3.2

攻防演练 offensive and defensive drills

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

3.3

PWN pwn

通过程序本身的漏洞，编写利用脚本破解程序拿到主机权限的形式。在 CTF 比赛中代表着溢出类的题目，其中常见类型的溢出漏洞有栈溢出、堆溢出。

3.4

CTF capture the flag

即夺旗比赛，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。参赛

队伍通过互联网，以在线环境交互或文件离线分析方式，解决网络安全技术挑战并获取相应分值。比赛结果根据选手所获总分和花费时间多少来排名。包括解题模式(Jeopardy)、攻防模式(AWD)，还有混合模式(Mix)赛制。

3.5

解题模式 jeopardy mode

在解题模式CTF赛制中，参赛队伍可以通过互联网或者现场网络参与，这种模式的CTF竞赛以解决网络安全技术挑战题目的分值和时间来排名，通常用于在线选拔赛。主要包含WEB、逆向、取证、隐写、密码、移动、二进制、PWN提权、杂项等。

3.6

攻防模式 attack with defense mode

在攻防模式CTF赛制中，参赛队伍在网络空间互相进行攻击和防守，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。攻防模式CTF赛制可以实时通过得分反映出比赛情况，最终也以得分直接分出胜负。

3.7

靶场演练 ISW

通过多个网络节点构建的对真实网络世界平行仿真的多层次，多路径的靶场场景，完成特定任务，并按完成时间和过程积分排名。

4 评定原则

4.1 自愿原则

在团队及成员自愿的基础上开展等级评定工作。

4.2 公开原则

团队的等级评定规则公开透明。

4.3 公平原则

采用统一、中立、持平的评定规则，以保证评定的公平性。

4.4 公正原则

评定的过程及其结果不受任何方的影响。

5 团队人员组成

团队可按网络安全攻防与应急实战演练、CTF 夺旗赛（解题模式、攻防模式、混合模式）靶场演练等赛事组成人员。

5.1 网络安全攻防与应急实战演练

由 3-5 名成员组成，可由渗透测试、WEB 安全、社会工程学等专业人员组成。

5.2 解题模式(Jeopardy)

由 3-6 名成员组成，可由 WEB、逆向、取证、隐写、密码、移动、二进制、流量数据分析、提权、漏洞挖掘等人员组成。

5.3 攻防模式(AWD)

由 3-5 名成员组成，可由若干名攻击和防守人员组成，一般需具备代码审计、攻击脚本编写、提权、后门维持、基线加固、流量监测、应急处置等能力的人员。

5.4 靶场演练(ISW)

由 4 名以内成员构成，需要具备综合网络安全渗透测试能力。利用各种网络安全技能，发现路径，实现角色任务。

6 团队的分级

团队等级分为一星级、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。具体的团队等级评定参见附录 A。

7 团队评价指标

7.1 基本条件

基本条件是评定团队等级的起评条件，申请等级认证的团队所有人员应拥护中国共产党的领导，拥护中国特色社会主义制度；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；应遵守相关法律法规的规定，无犯罪记录。团队人员还应具备攻防对抗、渗透测试等网络安全专业领域相关的经验。

7.2 管理制度要求

团队应由中国境内合法注册的企、事业单位或社会团体等组织批准成立，该组织承担对团队运作的管理责任。团队应具备人员及资产管理制度，技能合作训练、安全教育制度，漏洞攻击、渗透测试等方面的技能培训制度。此外，团队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。

7.3 能力要求

团队成员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。

7.4 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，其它重大创新竞赛或演练等。

7.5 业绩奖项

过去 2 年内，团队在相关比赛中获得荣誉奖项，可根据业绩奖项对团队进行等级评定。

8 团队的认证

团队的等级认证主要对基本条件、管理制度要求、能力要求、实战经验等指标进行评价，符合要求的团队可进行等级认证，颁发认证证书。

认证证书有效期为：2 年。有效期内每年应进行年审以确保团队符合等级要求，不满足年审要求的团队将受到黄牌警告，有严重问题的将取消认定证书。有效期满或人员调整后应进行延期评审或重新等级认定，根据认定结果调整等级。

9 团队评价方法

9.1 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 25 分，实战经验评价 20 分，业绩奖项评价 30 分。

评价计分细则见附录 A。

9.2 分数计算

总体评价分应按公式（1）计算：

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

式中：

S 一一总体评价分；

A 一一基本要求评价；

B 一一管理制度要求评价；

C 一一能力要求评价；

D 一一实战经验评价；

E 一一业绩奖项评价。

9.3 等级标准

总体评价分在 45 分及以上的，可获取一星级团队认证证书；

总体评价分在 55 分及以上的，可获取二星级团队认证证书；

总体评价分在 65 分及以上的，可获取三星级团队认证证书；

总体评价分在 75 分及以上的，可获取四星级团队认证证书；

总体评价分在 90 分及以上的，可获取五星级团队认证证书。

附 录 A
（规范性附录）
评价计分细则

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	制度一般 1 分 制度较好 2 分 制度完善 2.5 分
		专业的技能培训制度	制度一般 1 分 制度较好 2 分 制度完善 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
		不同获证人员的证书类别方向	单一类别 3 分 两种类别 5 分 三种类别 8 分 四种以上类别 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 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>
</table>

备注：

[1]赛事级别：

A 类赛：赛事主办方或指导单位级别为国家级，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

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。