ICS 35.110
CCS L 79

T/CSAC

团　　体　　标　　准

T/CSAC　XXX—XXXX

网络靶场 平台能力分级指南

Guide to capability grading of cyber range

（征求意见稿）

2023-03-15

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国网络空间安全协会　　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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国网络空间安全协会提出并归口。

本文件起草单位：鹏城实验室、广州大学网络空间先进技术研究院、哈尔滨工业大学(深圳)，中国信息通信研究院、北京永信至诚科技股份有限公司、电子科技大学、北京理工大学、中汽创智科技有限公司、广东为辰信息科技有限公司、重庆长安汽车股份有限公司、中国电信股份有限公司广东研究院、中国联合网络通信有限公司、中国移动通信集团有限公司、南方电网科学研究院有限责任公司、中国电子信息产业集团有限公司第六研究所、北京天融信网络安全技术有限公司、博智安全科技股份有限公司、中电长城网际系统应用有限公司

本文件主要起草人：贾焰，顾钊铨，罗翠，李树栋，胡宁，韩伟红，蔡晶晶，陈俊，李润恒，安伦，黄九鸣，杨明盛，周可，景晓，袁华平，陈元，余涛，关华，孟令逍，张静，林飞，罗蕾，赵焕宇，陈丽蓉，谢玮，孟楠，危胜军，杨彦召，薛信钊，汪向阳，王帅，金华敏，邱勤，王绍杰，傅涛，郑轶，徐天妮，陶冶，陈璐，李雪莹，王龑，匡晓云，杨祎巍，赵焕宇，燕玮，张凯，李炜。

网络靶场 平台能力分级指南

1 范围

本文件规定了网络靶场的主要功能、能力分级要求和平台能力分级规范。

本文件适用于指导网络靶场的设计、开发和建设，也适用于第三方机构对平台的综合能力进行审查和评估。

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。凡是不注日期引用文件，其最新版本（包括所有的修改单）适用于本文件。

YD/T 3644-2020 面向互联网的数据安全能力技术框架

2019-0981T-YD 网络安全空间仿真 术语

2022-0682T-YD 网络空间安全仿真 角色定义及功能规范

3 术语和定义

2019-0981T-YD 界定的以及下列术语和定义适用于本文件。

3.1

靶标 target

作为事态操作环境的一部分，在事态中作为攻击方的目标。它可以是软件、硬件、系统、平台环境等。

[来源：2019-0981T-YD]

3.2

分布式靶场 distributed cyber range

支持分布式试验的独立环境，能够独立自主完全实验；同时支持快速统一的互联互通，支持统一的试验管理和运行。

3.3

全局攻击 global attack

在联邦靶场中发生的攻击活动，从全局的角度分析攻击活动，一次全局攻击覆盖多个分布式靶场。

3.4

联邦制分布式靶场 federal distributed cyber range

简称联邦靶场，对具有层级式行政管理架构集团用户靶场建设，分布式靶场可采用联邦制，便于与其行政管理架构相匹配。其特点是可建立集中管控中心，对基础资源、试验资源、工具资源和试验项目、人员集中管控，优点是资源管理、调度和使用效率高，便于规划大型试验项目。

[来源：2019-0981T-YD]

3.5

有效攻击 effective attack

造成实际攻击后果的攻击活动。

[来源：2019-0981T-YD]

3.6

网络安全态势感知 network security situation awareness

通过感知网络环境来提取网络数据，并通过理解这些数据来评估网络安全状态，包括基础维、脆弱维、威胁维和综合维等网络安全态势。

4 概述

网络靶场是基于一组软硬件资源仿真一个目标网络，供给黄方、白方、红方、蓝方和绿方等主要的五方角色协同使用。仿真平台作为支撑网络攻防演练、网络完全技术测评、网络安全人才培养和网络新技术验证重大基础设置。五方角色协同完成试验，白方负责试验环境构建、红方负责攻击武器部署和攻防对抗、蓝方负责防御武器部署和攻防对抗、绿方负责攻防效果评估、黄方负责需求确定和任务想定等。靶场主要包括以下五大核心功能：

a) 导调指挥功能，负责试验中导演、指挥、资源调度和试验过程的统一管理。
b) 目标网络仿真与互联接入功能，提供整个试验的仿真环境，包括虚拟网络的生成、实物网络的配置，并在试验中提供环境状态监控和技术保障。
c) 攻击检测与态势评估功能，完成试验过程安全数据采集、攻击检测，并评估网络安全态势。
d) 攻击工具管理及组装部署功能，根据攻击方案完成攻击武器及技术部署。
e) 防御工具管理及协同运行功能，根据防御方案完成防御武器及技术部署。

5 网络靶场导调指挥能力分级

5.1 导调指挥功能

导调指挥功能供黄方使用，核心功能如下：

a) 靶场资源统一管理功能：支持靶场内资源统一管理，包括虚拟镜像资源、实体设备资源、靶标资源等。
b) 靶场试验过程半自动或手动管控功能：支持基于本地靶场的仿真环境构建，没有统一的试验任务启停、监控和指令下发等能力，试验过程控制通过半自动或手动完成。
c) 靶场试验过程自动化管控功能：支持本地靶场的试验过程的自动化管控，包括试验启动、监视和向白方、绿方、红蓝方等下达控制指令。
d) 分布式统一试验控制功能：支持分布式统一资源管理和试验控制，支持对分靶场的资源进行统一管理，支持接收来自联邦靶场的统一控制指令，并开展分布式试验任务，能够向其他分靶场等下发试验控制指令。

5.2 导调指挥能力分级

根据导调指挥功能需求，提出黄方系统能力分级：

第一级：具备靶场资源统一管理能力，不具备靶场试验过程管控功能，不具备分布式统一试验控制能力。

第二级：具备靶场资源统一管理能力和靶场试验过程半自动或手动控制能力，不具备分布式统一试验控制能力。

第三级：具备靶场资源统一管理能力和靶场试验过程自动化管控能力，不具备分布式统一试验控制能力。

第四级：具备靶场资源统一管理能力、靶场试验过程自动化管控能力、分布式统一试验控制能力。

6 目标网络仿真构建与互联接入能力

6.1 目标网络仿真构建

6.1.1 目标网络仿真构建功能

目标网络构建功能供白方使用，核心功能如下：

a) 单一场景的本地仿真功能：支持在本地靶场对固定场景进行仿真，场景可以是纯实物设备，也可以是一个固定的虚实结合场景。

b) 多个场景的本地仿真功能：支持利用本地靶场的有限资源按需构建不同的固定场景，仿真的场景固定不可编辑。

c) 自定义场景的本地仿真功能：支持基于本地靶场生成自定义的仿真场景，按需构建仿真场景。

d) 自定义场景的分布式协同仿真功能：支持通过自定义的方式构建分布式场景，能够接收联邦靶场的场景构建需求，并按需自动生成分布式场景，能够统一编排分靶场资源，支持构建分布式仿真场景。

6.1.2 目标网络仿真构建能力分级

根据仿真构建功能需求，提出白方系统仿真构建能力分级：

第一级：具备单一场景的本地仿真功能，不具备分布式协同仿真、自定义场景的本地仿真。

第二级：具备多个场景的本地仿真能力，不具备分布式协同仿真、自定义场景的本地仿真功能。

第三级：具备自定义场景的本地仿真、多个场景的本地仿真能力，不具备分布式协同仿真功能。

第四级：具备自定义场景的分布式协同仿真、自定义场景的本地仿真、多个场景的本地仿真能力。

6.2 互联接入

6.2.1 互联接入功能

互联接入功能供白方使用，核心功能如下：

a) 网络互联功能：支持不同靶场之间通过 TCP/IP 等方式实现网络层互联互通。

b) 资源互联功能：支持不同靶场之间进行数据和资源共享，可识别联邦靶场中其他靶场的业务数据、状态信息、资源状况等。

c) 分靶场场景互联功能：支持将已具备的场景与其他靶场进行互联。

d) 定制化场景互联功能：支持接收联邦靶场的统一控制，支持靶场多个自定义场景与其他靶场按需互联，并支持多场景安全隔离。

6.2.2 互联接入能力分级

根据互联接入功能需求，提出白方系统互联接入能力分级：

第一级：具备网络互联能力，不具备资源互联、分靶场场景互联和定制化场景互联能力。

第二级：具备网络互联、资源互联能力，不具备分靶场场景互联和定制化场景互联能力。

第三级：具备网络互联、资源互联和分靶场场景互联能力，不具备定制化场景互联能力。

第四级：具备网络互联、资源互联、分靶场场景互联和定制化场景互联能力。

7 攻防检测与态势评估能力

7.1 检测

7.1.1 攻击检测功能

攻击检测功能供绿方使用，核心功能如下：

a) 本地单步攻击检测功能：支持本地单步攻击行为检测，包括但不限于安全防护设备产生的单步攻击告警等形式。
b) 本地多步攻击检测功能：结合本地单步攻击数据支持本地多步攻击的检测。
c) 本地多步有效攻击检测功能：支持生成本地网络安全知识子图，通过资产和漏洞的关联关系去除无效攻击，支持本地多步有效攻击检测。
d) 全局有效攻击检测功能：针对分布式试验的攻击情况，支持生成全局网络安全知识子图，支持接收分靶场上传的攻击检测数据进行全局有效攻击的检测，支撑后续网络安全态势分析等。

7.1.2 攻击检测能力分级

根据攻击检测功能需求，提出绿方系统攻击检测能力分级要求：

第一级：具备本地单步攻击检测能力，不具备本地多步攻击检测、本地多步有效攻击检测、全局有效攻击检测能力。

第二级：具备本地单步攻击检测、本地多步攻击检测能力，不具备本地多步有效攻击检测、全局有效攻击检测能力。

第三级：具备本地单步攻击检测、本地多步攻击检测、本地多步有效攻击检测能力，不具备全局有效攻击检测能力。

第四级：具备本地单步攻击检测、本地多步攻击检测、本地多步有效攻击检测、全局有效攻击检测能力。

7.2 态势评估

7.2.1 态势评估功能

态势评估功能供绿方使用，核心功能如下：

a) 定性评估功能：根据攻击检测结果，支持对目标网络的安全态势进行定性评估，包括但不限于目标网络的资产状态、脆弱性、威胁识别等。
b) 定量评估功能：根据目标网络的资产、漏洞情况和攻击检测结果，支持对目标网络的安全态势进行定量评估，包括但不限于基础值、脆弱值、威胁值、综合值等网络安全态势指数。
c) 态势评估展示功能：根据定性、定量评估结果，支持对目标网络的安全态势指数进行可视化展示，包括但不限于图表等展示形式。
d) 实时量化评估功能：根据实时获取的目标网络的资产、漏洞情况和攻击检测结果，支持对目标网络的安全态势进行实时定量评估，包括但不限于基础值、脆弱值、威胁值、综合值等网络安全态势指数。
增加例子，

7.2.2 态势评估能力分级

根据态势评估功能需求，提出绿方系统态势评估能力分级：

第一级：具备定性评估能力，不具备定量评估、可视化展示、实时量化评估能力。

第二级：具备定性评估和定量评估能力，不具备可视化展示、实时量化评估能力。

第三级：具备定性评估、定量评估、可视化展示能力，不具备实时量化评估能力。

第四级：具备定性评估、定量评估、可视化展示、实时量化评估能力。

8 攻击工具管理及组装能力

8.1 攻击工具管理及组装功能

攻击工具管理、部署、组装及运行等功能供红方使用，包括攻击工具的资源管理，攻击工具的下发部署问题，实现面向联邦靶场的攻击工具选择、工具部署以及工具生命周期管理，核心功能如下：

a) 攻击工具管理功能：支持红方任务总览功能以及攻击工具的管理功能。

b) 攻击工具的本地部署与运行功能：支持在本地部署和运行攻击工具的功能，包括部署过程监控、攻击工具批量部署功能、部署环境管理、攻击工具自动/半自动运行等功能。

c) 攻击工具本地组装功能：支持按照设定的攻击流程对攻击工具进行本地组装，支持按需部署和运行攻击工具，包括攻击工具组装过程监控、环境管理等功能。

d) 攻击工具远程组装、部署和运行功能：支持攻击工具的远程组装、部署和运行，包括部署过程监控、攻击工具批量下载与部署、攻击工具按需组装、攻击工具自动/半自动运行等功能。

8.2 攻击工具管理及组装能力分级

根据攻击工具管理及组装功能需求，提出红方系统能力分级：

第一级：具备攻击工具管理能力，不具备攻击工具的本地组装部署与运行、攻击工具远程组装部署和运行能力。

第二级：具备攻击工具管理、攻击工具的本地部署与运行能力，不具备攻击工具的本地组装、攻击工具远程组装部署和运行能力。

第三级：具备攻击工具管理、攻击工具的本地组装部署与运行能力，不具备攻击工具远程组装部署和运行能力。

第四级：具备攻击工具管理、攻击工具的本地组装部署与运行、攻击工具远程组装部署和运行能力。

9 防御工具管理及协同运行能力

9.1 防御工具管理及协同运行功能

防御工具管理、部署、协同运行等功能供蓝方使用，包括防御工具的资源管理，防御工具的下发部署问题，实现面向联邦靶场的防御工具选择、工具部署、工具生命周期管理，核心功能如下：

a) 防御工具管理功能：支持蓝方任务总览功能以及防御工具的管理功能。

b) 防御工具的本地部署与运行功能：支持在本地部署和运行防御工具的功能，包括部署过程监控、防御工具批量部署功能、部署环境管理、防御工具自动/半自动运行等功能。

c) 防御工具本地协同运行功能：支持按照设定的防御流程对防御工具进行本地组装，支持按需部署和运行防御工具，包括防御工具协同运行及过程监控、环境管理等功能。

d) 防御工具远程部署及协同运行功能：支持防御工具的远程、部署及协同运行，包括部署过程监控、防御工具批量下载与部署、防御工具按需协同运行、防御工具自动/半自动运行等功能。

9.2 防御工具管理及协同运行能力分级

根据防御工具管理及协同运行功能需求，提出蓝方系统能力分级：

第一级：具备防御工具管理能力，不具备防御工具的本地部署及协同运行能力、防御工具远程部署及协同运行能力。

第二级：具备防御工具管理、防御工具的本地部署与运行能力，不具备防御工具本地协同运行、防御工具远程部署及协同运行能力。

第三级：具备防御工具管理、防御工具的本地部署及协同运行能力，不具备防御工具远程部署及协同运行能力。

第四级：具备防御工具管理、防御工具的本地部署与运行、防御工具远程部署及协同运行能力。

10 网络靶场能力分级参考

网络靶场能力分级可根据功能重要性进行分级。本文件根据仿真平台对导调指挥、目标网络仿真、互联接入、攻击检测、态势评估等方面的要求，对靶场能力分级。对于五方能力同等重要的仿真平台，能力分级参考表 1，如仿真平台能力为第三级，则五方系统的能力均需满足第三级，若某方系统能力超过第三级，可单独标注该方系统能力级别。

表 1 网络靶场能力分级参考

网络靶场能力分级	黄方	白方		绿方		红方	蓝方	说明
	导调指挥能力	仿真能力	互联能力	检测能力	评估能力	攻击工具管理及组装运行能力	防御工具管理及协同运行能力	
第四级	第四级	第四级	第四级	第四级	第四级	第四级	第四级	五方能力同等重要
第三级	第一级	第三级	-第二级	第二级-	第二级-	第二级-	第二级-	仿真类靶场
第二级	第一级-	-第一级	第一级-	第二级	第二级	第一级	第一级-	攻击检测评估类靶场
第一级	第一级	第一级	第一级	第一级	第一级	第一级	第一级	靶标接入类靶场

附 录 A
（资料性）

网络安全态势安全指数计算方案

A.1 概述

网络安全仿真验证平台从系统环境和攻击行为可将安全指数分为基础维、脆弱维和威胁维，并综合这三个维度的指数对系统整体进行评估，体现为综合维。

A.2 安全指数计算方案

A.2.1 基础维

基础维是反映试验环境中资产状态的指数，体现全网的基础状况。该指数与系统的初始状态指数和状态变化指数相关，计算公式如下：

基础维=初始状态指数+状态变化指数

A.2.1.1 初始状态指数

初始状态指数与试验环境的规模、环境中的节点类型以及节点的权重向量有关，通过响应的算法或者公式计算出初始状态指数，可参考如下计算方法和设置权重得到该指数。

初始状态指数 = Sum（B1*node_num），其中 B1 表示节点权重向量，node_num 表示拓扑里节点数量。

表 A.1 初始状态指数计算方案参考

应用类型	节点类型	说明	权重
互联网靶场	CLIENT	主机客户端	0.5
	SERVER	服务器	0.9
	DRT	动态路由	1
	FW	防火墙	1
	IDS	IDS	1
	IPS	IPS	1
	DES	DES	1
	WAF	WAF	1
	SW	二层交换机	0.5
	TSW	三层交换机	0.5
	PM	物理主机	0.6
	PR	物理路由	0.7
	PRT	公网路由	0.5
	FLAG	FLAG 服务器	0.3
工控-汽车远程升级	TBOX	车载远程信息处理器	0.9
	IVI	车机	0.8
	GATE	网关	0.4
	MMETER	仪表	0.5
	BaseStation	基站	0.9
工控-变电站	S-SERVER	变电站调度服务器	0.9
	ABB-CLIENT	ABB 工作站	0.8
	SIE-CLIENT	西门子工作站	0.8
	E-meter	智能电表	0.5
	R-FW	实物防火墙	0.7
	RTU	远程终端单元	0.4
	POWPROTECTION	变压器保护装置	0.3
	LINEPROTECTION	线路保护装置	0.5
	C ROTECTION	测控护装置	0.6

A.2.1.2 状态变化指数

状态变化指数由外界引起资产状态变化决定，主要是和环境的出入口流量相关，可参考如下计算方法和设置权重得到该指数。

状态变化指数 = B2*Flow+B3，其中 B2 表示降低系数（用于规约流量大小），B2 表示状态指数权重（根据流量大小判断），flow 为实时流量大小，单位为 Kb/s：

a) 当 flow∈(0,103]，B2=0.2，B3=0；

b) 当 flow∈(103,106]，B2=0.0002，B3=200；

c) 当 flow>106，B2=0. 00001，B3=400；

d) 若无法获取到流量，即 flow=0，则 B3 采用 range(5,100)范围内的随机变化指数。

A.2.2 脆弱维

脆弱维是反映试验环境中资产脆弱性的指数，体现全网脆弱性风险程度。其中漏洞是针对此工程环境，漏扫出来的漏洞数据，可参考以下计算公式得到该指数。

脆弱维 = v1 * 低危漏洞指数 + v2 * 中危漏洞指数 + v3 * 高危漏洞指数

其中 v1、v2、v3 表示权重值（如设置 v1=0.1，v2=0.3，v3=0.6），低危漏洞指数是系统扫描得到的低危漏洞数，中危漏洞指数是系统扫描得到的中危漏洞数，高危漏洞指数是系统扫描得到的高危漏洞数。

A.2.3 威胁维

威胁维是反映试验环境中资产受威胁程度的指数，体现全网受威胁程度。该系数与系统检测到的复杂攻击、有效攻击和基础攻击有关，可参考以下计算公式得到该指数。

威胁维 = t1 * 基础攻击指数 + t2 * 有效攻击指数 + t3 * 复杂攻击指数

其中 t1、t2、t3 表示权重值（如设置 t1=0.1，t2=0.3，t3=0.6），基础攻击指数是系统 1 秒内检测出的基础攻击总数，有效攻击指数是系统 1 秒内检测出的有效攻击总数，复杂攻击指数是系统 1 秒内检测出复杂攻击总数。

A.2.4 综合维

综合维是反映试验环境中总体情况的指数，体现全网综合态势。该系数与系统的基础维、脆弱维和威胁维三个系数相关，可参考一下公式得到该指数。

综合维 = c1 * 基础维 + c2 * 脆弱维 + c3 * 威胁维

其中 c1、c2、c3 表示权重值（如设置 c1=0.1，c2=0.3，c3=0.6），基础维、脆弱维和威胁纬是按照上述算法得到的各项参数值。

附 录 B
（资料性）基于应用模式的网络靶场能力分级

B.1 概述

网络靶场成功实践了四大应用模式，包括“内打内”、“内打外”、“外打内”及“外打外”。

内打内模式：立足网络靶场本身，开展网络人才培养和网络对抗演练。该模式可采用基于异域异构靶场的分布式竞赛环境，整合各独立建设的靶场资源形成特色资源共享，提供了稳定可靠的竞赛环境。

内打外模式：基于网络靶场，面向国家重大网络基础设施和系统，进行实网检测，有效支撑系列“护网”行动，实现了护网类评测的安全可控。

外打内模式：基于网络靶场，结合外部攻击资源，对重要信息产品进行安全测试，开拓了新型的网络安全评测方法，极大提升安全测试的科学性和时效性。

外打外模式：基于 IP 匿名映射技术，一方面实现对靶标真实 IP 的保护，一方面实现对攻击手必须通过靶场环境进行攻防操作的约束，有效支撑在线“护网”行动。

B.2 基于应用模式的网络靶场能力分级

表 B.1 基于内打内场景的网络靶场能力分级

网络靶场能力分级	黄方	白方		绿方		红方	蓝方
	导调指挥能力	仿真能力	互联能力	检测能力	评估能力	攻击工具管理及组装运行能力	防御工具管理及协同运行能力
第四级	第四级	第四级	第四级	第四级	第四级	第四级	不重点考虑
第三级	第三级	第三级	第三级	第三级	第三级	第三级	不重点考虑
第二级	第二级	第二级	第二级	第二级	第二级	第二级	不重点考虑
第一级	第一级	第一级	第一级	第一级	第一级	第一级	不重点考虑

表 B.2 基于内打外场景的网络靶场能力分级

网络靶场能力分级	黄方	白方		绿方		红方	蓝方
	导调指挥能力	仿真能力	互联能力	检测能力	评估能力	攻击工具管理及组装运行能力	防御工具管理及协同运行能力
第四级	第四级	不重点考虑	第四级	第四级	第四级	第四级	不重点考虑
第三级	第三级	不重点考虑	第三级	第三级	第三级	第二级-	不重点考虑
第二级	第二级-	不重点考虑	第二级	第二级	第二级	第二级	不重点考虑
第一级	第一级	不重点考虑	第一级	第一级	第一级	第一级	不重点考虑

表 B.3 基于外打内场景的网络靶场能力分级

网络靶场能力分级	黄方	白方		绿方		红方	蓝方
	导调指挥能力	仿真能力	互联能力	检测能力	评估能力	攻击工具管理及组装运行能力	防御工具管理及协同运行能力
第四级	第四级	第四级	第四级	第四级	第四级	第四级	不重点考虑
第三级	第三级	第三级	第三级	第三级	第三级	第二级	不重点考虑
第二级	第二级	第二级	第二级	第二级	第二级	第二级	不重点考虑
第一级	第一级	第一级	第一级	第一级	第一级	第一级	不重点考虑

表 B.4 基于外打外场景的网络靶场能力分级

网络靶场能力分级	黄方	白方		绿方		红方	蓝方
	导调指挥能力	仿真能力	互联能力	检测能力	评估能力	攻击工具管理及组装运行能力	防御工具管理及协同运行能力
第四级	第四级	第四级	第四级	第四级	第四级	第四级	不重点考虑
第三级	第三级	第三级	第三级	第三级	第三级	第二级	不重点考虑
第二级	第二级	第二级	第二级	第二级	第二级	第二级	不重点考虑
第一级	第一级	第一级	第一级	第一级	第一级	第一级	不重点考虑