



中华人民共和国国家标准

GB/T 46820—2025

网络安全技术 网络安全试验平台 体系架构

Cybersecurity technology—Cybersecurity experiment platform—Architecture

2025-12-02 发布

2026-07-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 1

5 概述 2

6 总体架构 2

7 组件功能 3

 7.1 目标网络构建组件 3

 7.2 攻防管理组件 4

 7.3 试验管理组件 4

 7.4 试验监测与评估组件 5

 7.5 多平台互联组件 6

附录 A（资料性） 网络安全试验过程 7

参考文献 10

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。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：鹏城实验室、广州大学、国家计算机网络应急技术处理协调中心、中国电信股份有限公司研究院、国网江西省电力有限公司、中汽研汽车检验中心(天津)有限公司、中汽创智科技有限公司、重庆长安汽车股份有限公司、中国信息通信研究院、北京中关村实验室、中国移动通信集团、中国移动通信集团设计院有限公司、四川亿览态势科技有限公司、软极网络技术(北京)有限公司、北京天融信网络安全技术有限公司、奇安信科技集团股份有限公司、北京安天网络安全技术有限公司、北京邮电大学、哈尔滨工业大学(深圳)、北京理工大学、塔里木大学、中移物联网有限公司、南方电网科学研究院有限责任公司、国网新疆电力有限公司电力科学研究院、山东省计算中心(国家超级计算济南中心)、中国信息安全测评中心、国家工业信息安全发展研究中心、国网山东省电力公司电力科学研究院、中国工程物理研究院计算机应用研究所、兴唐通信科技有限公司、数字湖南有限公司、中石化安全工程研究院有限公司、新华三技术有限公司、杭州安恒信息技术股份有限公司、南京赛宁信息技术有限公司、永信至诚科技集团股份有限公司、北京神州绿盟科技有限公司、北京时代新威信息技术有限公司、博智安全科技股份有限公司、陕西省信息化工程研究院、西安交大捷普网络科技有限公司、广东为辰信息科技有限公司、广东电网有限责任公司信息中心、广东盈世计算机科技有限公司、陕西省网络与信息安全测评中心、中科信息安全共性技术国家工程研究中心有限公司、蓝象标准(北京)科技有限公司、内蒙古工业大学、启明星辰信息技术集团股份有限公司、北京山石网科信息技术有限公司。

本文件主要起草人：贾焰、李树栋、韩伟红、胡宁、顾钊铨、向文丽、郑志彬、刘欣然、王帅、金华敏、邱日轩、王钢、李润恒、王文磊、田志宏、殷丽华、安伦、付玉龙、张立武、谢玮、王东滨、贺可勋、杨彦召、李峰、赵大伟、张家伟、陈德伟、邱欣逸、景晓、梅阳阳、郑涛、余涛、向夏雨、孟令道、罗翠、李宗哲、陶莎、崔牧凡、董航、张高山、于雷、徐鹏、王龔、刘利军、高坤、刘勇、孟楠、汪向阳、孙娅苹、郭超、赵超、危胜军、梁志宏、刘新、杨祎巍、沈伍强、冯永胜、殷明勇、谢家俊、万晓兰、俞政臣、郑轶、胡志锋、张勇、何建锋、陈丽蓉、苗春雨、张超、胡建勋、宋诚、林延中、胡吉祥、陈俊、孟琦、王国伟、曹德舜、肖岩军、张红艳、胡月、吴疆、燕玮、杨天识。

网络安全技术

网络安全试验平台 体系架构

1 范围

本文件确立了网络安全试验平台的体系架构,包括总体架构、组件功能。
本文件适用于网络安全试验平台的设计、开发与建设。

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于本文件;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。

- GB/T 20986 信息安全技术 网络安全事件分类分级指南
- GB/T 22239 信息安全技术 网络安全等级保护基本要求
- GB/T 25069 信息安全技术 术语
- GB/T 25070 信息安全技术 网络安全等级保护安全设计技术要求

3 术语和定义

GB/T 25069、GB/T 20986 界定的以及下列术语和定义适用于本文件。

3.1

网络安全试验 cybersecurity experiment

在仿真环境中开展的网络安全技术验证、网络安全能力测试与评估、网络攻防演练等试验活动。

注:本文件中作为组合词出现时又简称为试验或试验任务。

3.2

网络安全试验平台 cybersecurity experiment platform

为开展网络安全试验提供所需运行环境的信息系统。

3.3

目标网络 target network

根据试验需求,运用虚拟、实物与模拟等建模技术在网络安全试验平台上构建的仿真网络。

注:根据试验需求,目标网络包括用于支撑试验活动的虚拟或实物的靶标设备、攻击设备、跳板设备、防护设备等,以及连接各设备的网络设备及网络链路;目标网络也包括所模拟的网络行为。

4 缩略语

下列缩略语适用于本文件。

ATT&CK:对抗战术、技术和常识(Adversarial Tactics, Techniques and Common Knowledge)

CAPEC:公共攻击模式枚举和分类(Common Attack Pattern Enumeration and Classification)

CNNVD:国家信息安全漏洞库(China National Vulnerability Database of Information Security)