



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)

CNVD:国家信息安全漏洞共享平台(China National Vulnerability Database)

CPE:通用平台枚举(Common Platform Enumeration)

CVE:通用漏洞和披露(Common Vulnerabilities and Exposures)

CWE:通用弱点枚举(Common Weakness Enumeration)

NVDB:网络安全威胁和漏洞信息共享平台(National Vulnerability DataBase)

5 概述

网络安全试验平台通过仿真开展网络安全试验所需的支撑环境,开展网络安全技术验证、网络安全能力测试与评估、网络攻防演练等试验活动,并与其他网络安全试验平台互联共享资源,以支撑不同类型的网络安全试验。

网络安全试验平台的用户是操作和使用网络安全试验平台的人员。用户分为以下类型。

- a) 目标网络构建方:目标网络的构建和维护者。
- b) 攻击方:网络攻击活动的发起方。
- c) 防御方:网络攻击活动的应对方。
- d) 导调方:网络安全试验的设计者和组织者。
- e) 评估方:网络安全试验的评估者。



6 总体架构

网络安全试验平台的总体架构包括目标网络构建组件、攻防管理组件、试验管理组件、试验监测与评估组件、多平台互联组件,如图 1 所示。根据实际需要,平台可选择构建以下对应组件。

- a) 目标网络构建组件:通过虚拟化网络设备及链路、实物设备接入虚拟网络、模拟网络行为等方法,构建用于开展网络安全试验活动的目标网络。目标网络构建方通过该组件构建和维护目标网络。
- b) 攻防管理组件:管理网络安全试验平台的攻防工具及攻防过程。攻击方通过该组件对靶标发起攻击,防御方通过该组件防御攻击行为。
- c) 试验管理组件:规划和控制网络安全试验活动的过程,归档试验结果。导调方通过该组件制定试验需求和试验计划、控制试验过程。
- d) 试验监测与评估组件:监测网络安全试验平台上开展试验的过程,评估试验过程中的安全事件。评估方通过该组件监测和评估网络安全试验活动的攻防行为。
- e) 多平台互联组件:根据试验需求,为目标网络构建组件、攻防管理组件、试验管理组件、试验监测与评估组件与其他网络安全试验平台的互联提供统一接口。

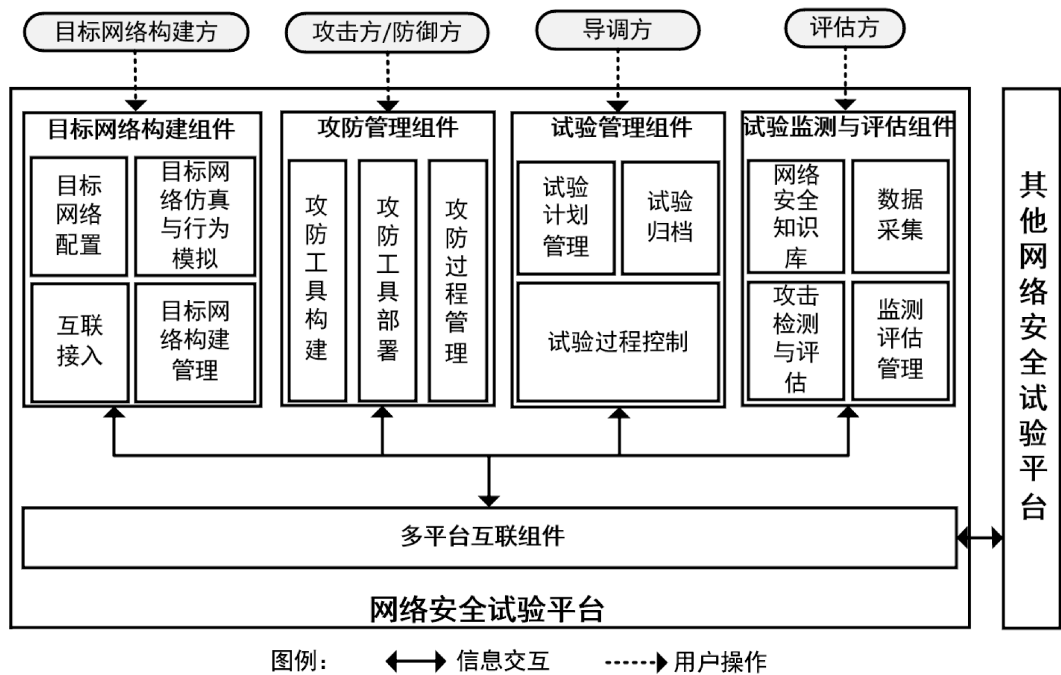


图 1 网络安全试验平台总体架构

网络安全试验平台构建应符合 GB/T 22239、GB/T 25070 的相关要求,从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理方面进行安全性设计。

网络安全试验过程见附录 A。通过完整的试验过程对网络安全试验平台的组件、用户以及信息交互进行了描述。

7 组件功能

7.1 目标网络构建组件

7.1.1 目标网络配置

- 目标网络配置包括以下功能。
- a) 目标网络编排:编排试验所需的目标网络的拓扑结构,包括节点、节点之间的连接关系。其中节点包括虚拟设备节点、实物设备节点等类型。
 - b) 资源调度:根据编排的目标网络,调度虚实资源,将目标网络拓扑下发到目标网络仿真与行为模拟模块。

7.1.2 目标网络仿真与行为模拟

- 目标网络仿真与行为模拟包括以下功能。
- a) 网络和设备虚拟化:运用虚拟化技术将配置的目标网络拓扑结构进行虚拟化,构建虚拟网络;根据试验需求对服务器、路由器、防火墙等设备节点进行虚拟化仿真,并接入到虚拟网络中;为攻防管理组件提供目标网络虚拟设备的入口;为试验监测与评估组件提供流经虚拟网络的流量。
 - b) 数据通道:为虚拟网络内指定的设备节点建立受控的数据传输通道,向试验监测与评估组件、攻防管理组件传输节点内的运行数据。

- c) 网络行为模拟:在目标网络环境中模拟真实的网络行为。

7.1.3 互联接入

互联接入包括以下功能。

- a) 靶标接入:将靶标接入所构建的目标网络环境中,扩充目标网络环境的功能。
- b) 目标网络互联:将多个目标网络进行互联,扩充目标网络规模。

7.1.4 目标网络构建管理

目标网络构建管理包括以下功能。

- a) 设备管理:管理虚拟设备节点、实物设备节点以及用于目标网络仿真与行为模拟的硬件设施。
- b) 任务管理:管理目标网络构建任务的准备、开始、结束、归档等。

7.2 攻防管理组件

7.2.1 攻防工具构建

攻防工具构建包括以下功能。

- a) 工具资源管理:构建攻防工具库,管理和维护攻防工具。
- b) 工具推荐:为攻击方、防御方推荐攻防工具。

7.2.2 攻防工具部署

攻防工具部署包括以下功能。

- a) 权限与任务管理:根据试验任务,为攻击方、防御方分配攻防工具的使用权限,并监控攻防工具的部署过程和运行状态。
- b) 攻防工具部署:攻击方、防御方部署所选择的攻防工具。

7.2.3 攻防过程管理

攻防过程管理包括以下功能。

- a) 攻防入口管理:通过目标网络构建组件提供目标网络设备入口,管理攻击方和防御方接入攻击设备与靶标设备。
- b) 攻防过程监控:通过运行在目标网络设备节点中的监控服务等方式监控攻击方、防御方的攻防过程,控制攻击产生的损害程度。
- c) 攻防结果管理:记录并管理攻击方、防御方的攻防结果。
- d) 攻防任务管理:负责接收试验管理组件的控制指令,管理攻防任务的准备、开始、结束、归档等。

7.3 试验管理组件

7.3.1 试验计划管理

试验计划管理包括以下功能。

- a) 计划生成:根据网络安全技术验证、网络安全能力测试与评估、网络攻防演训等试验活动的需要,生成试验的计划方案,包括试验的类型、试验参与人员、目标网络构建计划、攻防计划、试验监测与评估计划、平台互联计划等。
- b) 计划配置:在试验前配置试验计划中的各个步骤和任务。

7.3.2 试验过程控制

试验过程控制包括以下功能。

- a) 试验控制:将试验的准备、开始、结束等控制指令下发给目标网络构建组件、试验监测与评估组件、攻防管理组件,根据试验计划控制试验过程。
- b) 试验监测:监测试验运行过程中目标网络构建组件、试验监测与评估组件、攻防管理组件的任务状态。

7.3.3 试验归档

试验归档包括以下功能。

- a) 数据归档:通知目标网络构建组件、试验监测与评估组件、攻防管理组件对试验数据进行归档,并统计相关的归档数据。
- b) 资源释放:通知目标网络构建组件、试验监测与评估组件、攻防管理组件释放占用的试验资源。

7.4 试验监测与评估组件

7.4.1 网络安全知识库

网络安全知识库的功能包括构建、管理及维护以下知识。

- a) 攻击行为知识:包括检测到的攻击行为、ATT&CK、CAPEC 等知识。
- b) 漏洞知识:描述漏洞数据及其关联的弱点信息,包括 NVDB、CNVD、CNNVD、CVE、CWE 等漏洞库包含的知识。
- c) 资产知识:对资产信息进行标准化描述的知识,包括 CPE 等知识。
- d) 资产、漏洞、攻击行为关联的知识:包括资产与漏洞关联的知识、资产与攻击行为关联的知识、攻击行为与漏洞关联的知识。

7.4.2 数据采集

数据采集包括以下功能。

- a) 流量数据采集:采集目标网络中传输的流量等信息。
- b) 日志数据采集:通过运行在目标网络设备节点中的探针等方式采集目标网络中计算机或网络设备的系统操作、用户活动行为等日志信息。
- c) 资产数据采集:采集目标网络中计算机或网络设备的硬件、软件资源信息。
- d) 漏洞数据采集:采集目标网络中硬件、软件等资产存在的漏洞信息。

7.4.3 攻击检测与评估

攻击检测与评估包括以下功能。

- a) 网络攻击检测:利用采集的数据,检测试验中产生的单步攻击行为、多步攻击行为。
- b) 攻击研判:基于网络攻击检测结果及网络安全知识进行关联分析,建立安全事件之间的因果关系,还原攻击过程,研判攻击意图。
- c) 评估:针对网络安全技术验证活动,评估网络安全技术的效能;针对网络安全能力测试与评估活动,评估网络安全攻击能力、防御能力等;针对网络攻防演练活动,评估演练过程的风险与影响,以及相关能力水平。
- d) 攻防可视化:根据攻击行为、防御行为以及资产状态变化,展示网络安全试验过程中的攻防态势。

7.4.4 监测评估管理

监测评估管理包括以下功能。

- a) 设备管理:管理网络安全试验平台中的数据采集、攻击检测与评估等的软硬件设备。
- b) 任务管理:负责接收试验管理组件的控制指令,管理试验监测与评估任务的准备、开始、结束、归档等。

7.5 多平台互联组件

多平台互联组件实现将多个网络安全试验平台互联,按照互联的能力水平从低到高,包括基础网络、业务数据、资源控制和任务协同四个方面的互联。

- a) 基础网络互联:为多个网络安全试验平台的基础物理网络提供网络层互联功能,实现网络层通信。
- b) 业务数据互联:为多个网络安全试验平台提供统一的业务数据交换通道,安全传输多个网络安全试验平台之间的业务数据。
- c) 资源控制互联:为多个网络安全试验平台提供统一的资源管理和控制接口,调度和编排多个网络安全试验平台的计算、存储和网络等资源。
- d) 任务协同互联:为多个网络安全试验平台提供统一的试验任务描述接口,设计与编排多个网络安全试验平台协同参与的任务。



附录 A
(资料性)
网络安全试验过程

网络安全试验过程按照试验的状态分为试验准备阶段、试验运行阶段、试验后处理阶段。

- a) 试验准备阶段的试验过程如图 A.1 所示,包括以下工作。
- 1) 导调方将本次试验需求通过试验管理组件进行配置,形成试验计划(见图 A.1 步骤 a1)。
 - 2) 多平台互联组件的工作:多平台互联组件根据试验需求,为目标网络构建组件、攻防管理组件、试验管理组件、试验监测与评估组件与其他网络安全试验平台的互联提供统一接口,实现多个网络安全试验平台互联(见图 A.1 步骤 a2)。
 - 3) 目标网络构建组件的工作:试验管理组件根据试验计划对目标网络构建组件下达试验准备指令,并将试验相关信息同步至目标网络构建组件。目标网络构建组件配置、仿真本次试验的网络拓扑,并将相关准备信息返回给试验管理组件(见图 A.1 步骤 a3)。
 - 4) 试验监测与评估组件的工作 1:试验管理组件收到目标网络构建组件返回的准备完成指令后,根据试验计划对试验监测与评估组件下达试验准备指令,并将试验相关信息同步至试验监测与评估组件。试验监测与评估组件进行数据采集配置、攻击检测配置等,并将相关准备信息返回给试验管理组件(见图 A.1 步骤 a4)。
 - 5) 试验监测与评估组件的工作 2:试验监测与评估组件从目标网络构建组件获取仿真的准备数据(见图 A.1 步骤 a5)。
 - 6) 攻防管理组件的工作 1:试验管理组件收到目标网络构建组件返回的准备完成指令后,根据试验计划对攻防管理组件下达试验准备指令,并将试验相关信息同步至攻防管理组件(见图 A.1 步骤 a6)。
 - 7) 攻防管理组件的工作 2:攻防管理组件从目标网络构建组件获取目标网络设备的入口、对本次试验的虚拟机预置攻防工具部署服务(见图 A.1 步骤 a7)。

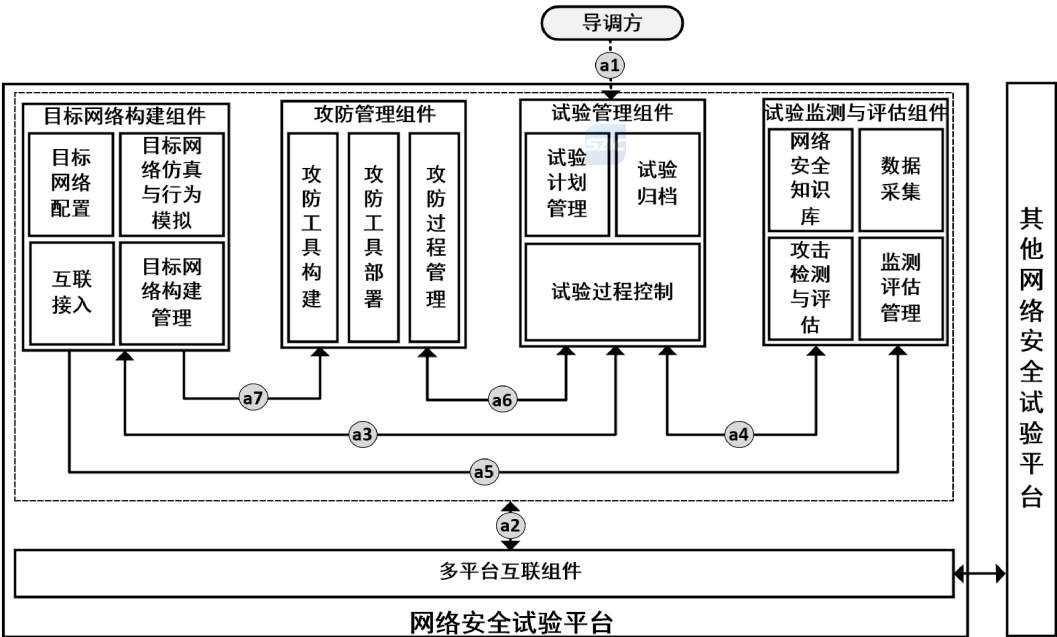


图 A.1 网络安全试验平台的试验准备阶段

b) 试验运行阶段的试验过程如图 A.2 所示,包括以下工作。

- 1) 导调方对试验管理组件发送试验开始请求(见图 A.2 步骤 b1)。
- 2) 目标网络构建组件的工作:试验管理组件对目标网络构建组件下达试验开始指令,目标网络构建组件进行网络行为模拟,监控目标网络设备节点的状态(见图 A.2 步骤 b2)。
- 3) 试验监测与评估组件的工作 1:试验管理组件对试验监测与评估组件下达试验开始指令,试验监测与评估组件进行数据采集、攻击检测与评估(见图 A.2 步骤 b3)。
- 4) 试验监测与评估组件的工作 2:试验监测与评估组件从目标网络构建组件获取目标网络的运行数据(见图 A.2 步骤 b4)。
- 5) 攻防管理组件的工作 1:试验管理组件对攻防管理组件下达试验开始指令,攻防管理组件生成攻防武器部署方案、部署攻防工具及过程监控、控制攻防过程、管理攻防结果(见图 A.2 步骤 b5)。
- 6) 攻防管理组件的工作 2:攻防管理组件从目标网络构建组件获取目标网络设备的入口等服务(见图 A.2 步骤 b6)。
- 7) 攻防管理组件的工作 3:攻击方和防御方接入目标网络设备进行试验操作(见图 A.2 步骤 b7)。

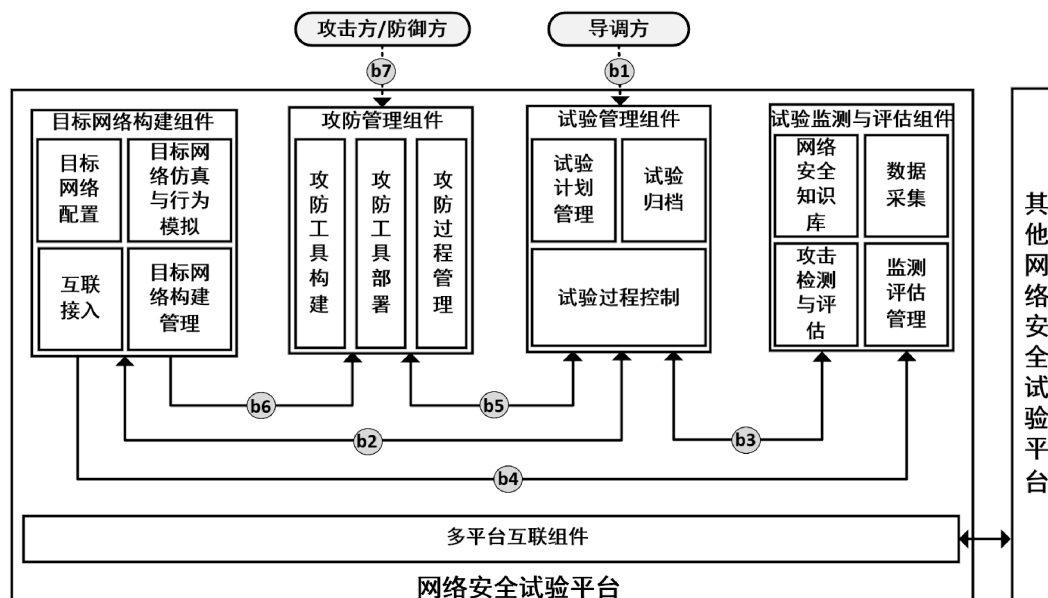


图 A.2 网络安全试验平台的试验运行阶段

c) 试验后处理阶段的试验过程如图 A.3 所示,包括以下工作。

- 1) 导调方对试验管理组件发送试验停止请求(见图 A.3 步骤 c1)。
- 2) 目标网络构建组件的工作:试验管理组件对目标网络构建组件下达试验停止指令,目标网络构建组件清空网络拓扑资源,归档试验数据并回传至试验管理组件(见图 A.3 步骤 c2)。
- 3) 试验监测与评估组件的工作:试验管理组件对试验监测与评估组件下达试验停止指令,试验监测与评估组件停止数据采集、攻击检测与评估,更新网络安全知识库,归档试验数据并回传至试验管理组件(见图 A.3 步骤 c3)。
- 4) 攻防管理组件的工作:试验管理组件对攻防管理组件下达试验停止指令,攻防管理组件关闭攻击方和防御方的网络节点接入入口,清除部署在目标网络虚拟机上的攻防工具,归档试验数据并回传至试验管理组件(见图 A.3 步骤 c4)。

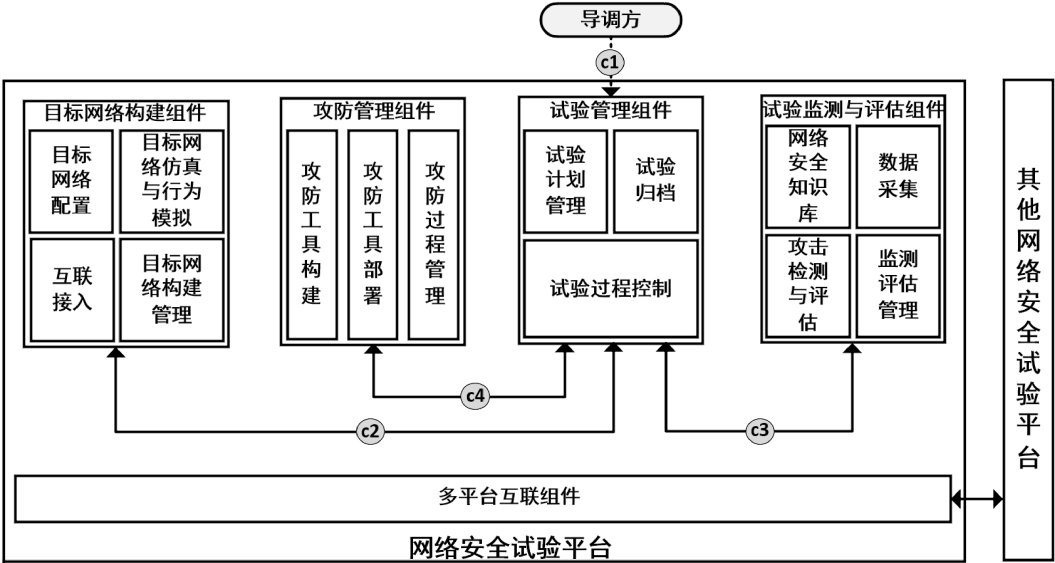


图 A.3 网络安全试验平台的试验后处理阶段

在试验全过程中,目标网络构建方与评估方负责运维管理工作,如图 A.4 所示。目标网络构建方负责进行目标网络构建组件的构建运维管理(见图 A.4 步骤 d),评估方进行试验监测与评估组件的评估运维管理(见图 A.4 步骤 e)。

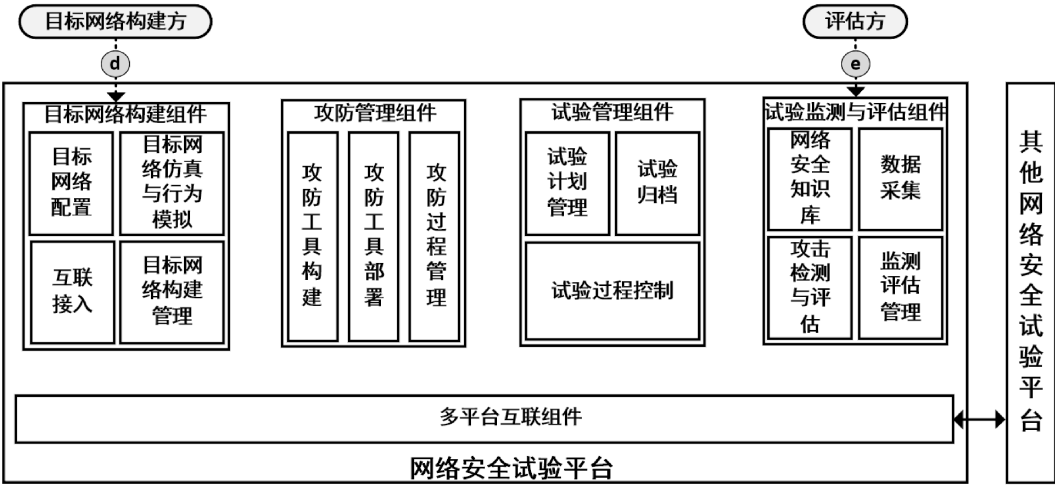


图 A.4 网络安全试验平台的运维管理工作

参 考 文 献

- [1] YD/T 4588—2023 网络空间安全仿真 参考架构
 - [2] YD/T 4593—2023 网络空间安全仿真 平台试验操作要求
-

