ICS 35.240.95
CCS L 67

YD

中华人民共和国通信行业标准

YD/T XXXXX—XXXX

网络空间安全仿真 运行控制技术要求

Cybersecurity emulation — Run-time control technical requirements

报批稿

XXXX－XX－XX 发布 XXXX－XX－XX 实施

中华人民共和国工业和信息化部 发布

目　　次

前　言

本文件按照GB/T1.1-2020《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。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：中电长城网际安全技术研究院（北京）有限公司、鹏城实验室、广州大学网络空间先进技术研究院、北京邮电大学。

本文件主要起草人：林飞、张晓刚、鲁明明、李树栋、贾焰、田志宏、韩伟红、王东滨。

网络空间安全仿真　运行控制技术要求

1　范围

本文件规定了在网络空间安全仿真系统或产品中运行控制部分的功能、性能、环境和安全的技术要求。

本文件适用于指导网络空间安全仿真中运行控制部分的设计、开发、建设、部署。

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。

GB/T 25069-2010 信息安全技术 术语

3　术语和定义

GB/T 25069-2010界定的以及下列术语和定义适用于本文件。

3.1

运行控制 run-time control

在网络空间安全仿真系统的试验运行过程中，系统对网络空间安全仿真试验的各种控制功能。

3.2

试验模拟数据 experiment simulated data

由网络空间安全仿真系统导入到试验环境中的数据，该数据用于配合试验，包括背景流量、前景流量等模拟数据等。

4　概述

如图1所示，本文件分别从四个层面对网络空间安全仿真运行控制部分进行技术要求，功能技术要求包括：试验准备、试验控制、试验环境控制、试验评估控制的要求。性能技术要求包括：试验环境性能、试验采集性能、试验环境仿真度和试验控制响应性能的要求。环境技术要求包括：运行控制介质和陪试环境的要求。安全技术要求包括：安全审计和应急响应的要求。

图1　网络空间安全仿真运行控制技术要求结构图

5　功能技术要求

5.1　试验准备功能要求

试验准备是运行控制前提保障，保障正式运行前试验已经准备就绪。包括以下四项准备：

a）应支持显示试验环境是否准备就绪的功能，扩展可支持发起试验环境准备检查和提交试验环境准备检查结果功能；

b）应支持显示试验人员是否准备就绪的功能，扩展可支持发起试验人员准备检查和提交试验人员准备检查结果功能；

c）应支持显示试验模拟数据是否准备就绪的功能，扩展可支持发起试验模拟数据准备检查和提交试验数据准备检查结果功能；

d）应支持显示试验资源数据是否准备就绪的功能，扩展可支持发起试验资源数据准备检查和提交试验资源数据准备检查结果功能。

5.2　试验控制功能要求

试验控制功能是运行控制中以试验为单位的控制功能，以便控制试验进程。包括以下六项功能：

a）应支持试验开始的功能，试验开始后试验进入实施阶段；准备尚未就绪的需要提示，也可以忽略提示，依旧开始试验；

b）应支持试验终止的功能，试验终止功能将停止试验，试验停止后试验暂停、试验继续、试验保存、试验回滚和试验环境控制功能不再可用，进入试后处理阶段；

c）应支持试验暂停和试验继续功能，该功能只能在试验实施阶段使用，试验暂停功能将暂停试验环境中所有节点以及试验数据，试验继续功能将试验环境恢复到试验暂停前的状态；

d）应支持试验保存和试验回滚功能，该功能只能在试验实施阶段使用，试验保存功能将保存试验环境中所有虚拟机节点的磁盘数据，亦可保存内存数据；试验回滚可选择已经保存的进行批量恢复；

e）应支持试验归档功能，该功能只能在试后处理阶段使用，试验归档功能将试验环境、试验运行中产生的数据进行离线保存，以便后续的提取，试验运行中产生的数据包括试验保存的场景快照、节点快照、采集数据、模拟数据等。

f）应支持试验提取功能，试验提取功能将从归档中适当选取数据、信息重新投入到试验中。

5.3　试验环境控制功能要求

试验环境控制功能是运行控制中对指定的试验环境进行控制，以便在实施阶段调整试验环境。包括以下六项功能：

a）应支持对试验节点的控制功能，包括对节点的开机、关机、暂停、继续、保存快照、恢复快照功能，以及获取或显示节点的状态的功能；

b）应支持对试验拓扑的控制功能，包括修改网络拓扑结构、调整节点规格配置、调整链路的带宽、调整链路的延迟功能；

c）应支持对试验采集的控制功能，包括修改指定节点的采集策略、启停指定节点的采集；

d）应支持对试验数据的控制功能，包括播放、停止播放指定背景流量数据，播放、停止播放指定前景流量数据，选用指定工具生成模拟数据的功能；

e）应支持对试验应用的控制功能，包括部署指定应用、运行指定应用、停止指定应用和卸载指定应用；

f）应支持对试验安全的控制功能，包括试验的隔离控制、试验节点权限的控制；试验的隔离控制需要至少支持试验间的隔离，可扩展支持打通试验间的通路功能；

5.4 试验评估控制功能要求

试验评估控制功能是运行控制中控制不同使用角色的展示内容，以便不同角色更直观的控制试验。包括以下两项功能：

a）应支持展示内容设计功能，展示内容设计为针对不同运行控制使用角色设计不同的展示内容的功能，具体展示内容不做要求；

b）应支持分析方式控制功能，分析方式控制为运行控制角色对运行时分析工具、脚本具有调整控制的功能，具体分析工具和脚本不做要求。

6 性能技术要求

6.1 试验环境性能要求

试验环境性能要求是运行控制中对试验环境的可靠性和环境重现能力的要求。包括以下两项功能：

a）试验环境运行可靠性不低于99.9%；

b）试验环境重现至少可以还原所有虚拟化部分的网络结构、节点镜像，可扩展升级还原部分实物设备、虚拟网络节点的配置、虚拟主机的内存数据。

6.2 试验采集性能要求

试验采集性能要是运行控制中对试验中可以控制的采集项、规则配置能力，以及采集数据传输模式和传输速率的性能要求。包括以下四项功能：

a）应支持对试验节点中的采集配置实时修改、实时生效；

b）采集代理的运行模式至少包含带外采集和带内采集中的一种；

c）带内采集的数据需要采用带外传输的模式，即不占用虚拟机的网卡进行传输数据。

d）采集数据传输速率不低于100MB/s；

6.3 试验环境仿真度要求

试验环境仿真度要求是指运行控制部分应明确显示的指出当前试验环境、节点所处的仿真度的级别。如图2所示，仿真度级别分为设施仿真、资源仿真、协议仿真、功能仿真和数据仿真：

图2　网络空间安全仿真运行控制仿真度层次图

a）设施仿真，仿真程度最高的仿真，对硬件进行仿真，采用设施的镜像形成与物理设施的物理特性、操作特性、功能特性、协议特性基本一致的仿真；

b）资源仿真，仿真程度较高的仿真，基本采用设施的镜像，形成与物理设施的操作特性、功能特性、协议特性基本一致的仿真；

c）协议仿真，仿真程度一般的仿真，使用模拟程序模拟功能协议，形成与物理设施的功能特性、协议特性基本一致的仿真；

d）功能仿真，仿真程度一般的仿真，使用模拟程序模拟功能，不具备设施的协议，仅与物理设施的功能特性基本一致的仿真；

e）数据仿真，仿真程度较低的仿真，使用模拟程序模拟数据，在特殊情况下较为有用，如模拟车速、天气、地震，一般与其他设施配套使用，提供模拟的客观参数等。

6.4　试验控制响应性能

试验控制响应性能要是运行控制中对试验控制指令、试验状态信息、试验数据转发的要求。包括以下五项功能：

a）试验控制指令下发的延迟不得高于1ms；

b）试验状态信息推送的延迟不得高于1ms；

c）试验数据转发的延迟不得高于1ms；

d）试验状态信息推送应支持同时向多个地址推送信息，至少可同时向2个地址推送信息；

e）试验数据转发应支持同时向多个地址转发数据，至少可同时向2个地址转发数据；

7　环境技术要求

7.1　运行控制介质

运行控制介质要是运行控制模块对运行环境的要求。至少支持脑机控制、声光控制、触摸控制、手势控制、键鼠控制中的一种，可扩展支持其他介质；

多种控制介质可同时使用进行控制。

7.2　陪试环境

陪试环境是对试验环境中陪伴主要测试模块进行测试使用的环境，可以是虚拟环境，也可以是物理环境。包括以下三项要求：

a）陪试环境应具备可用性检查，支持周期性检查和指令检查；

b）陪试环境其可靠性不低于99%，且出现问题后，不应对试验环境造成破坏影响；

c）陪试环境应具备完备性，陪试环境部分出现问题可以进行替换，替换后不影响使用；

8 安全与应急技术要求

8.1 安全审计要求

包括以下要求：

a）运行控制过程中，要对攻防双方的操作进行事实记录，以便做事后审计；

b）对运行控制的安全审计记录应准确、全面、存储稳定、可控读取。

8.2 应急响应要求

对于以在线运行或重要的行业应用系统为靶标的网络空间安全仿真应用系统，在活动启动前应满足相应的应急响应技术要求，主要包括应急监测、应急预案、应急响应流程、应急专家支撑等环节。包括以下要求：

a）应具备应急事件实时监测功能，其监测项可配置，事件内容可获取；

b）应急监测事件可订阅与推送，可推送到：

——指定响应负责人；

——已注册的应急专家；

——其他应急处置人。

c）应具备应急预案，运行前要制定相应的应急预案，可保存在电子或纸质介质上；

d）应急处置完毕后，应形成应急处置报告，并保存在电子或纸质介质上。