ICS 35.110
CCS M 11

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 资源管理库技术架构

Cyberspace security simulation — Resource management library technology architecture

（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/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。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：杭州安恒信息技术股份有限公司、鹏城实验室、广州大学网络空间先进技术研究院、贵州国卫信安科技有限公司、哈尔滨工业大学（深圳）、四川亿览态势科技有限公司、软极网络技术（北京）有限公司、湖南星汉数智科技有限公司、郑州信大捷安信息技术股份有限公司、新华三技术有限公司。

本文件主要起草人：苗春雨、叶章龙、贾焰、田丽丹、林明峰、钱晓斌、唐玮涛、李树栋、陶莎、陈星、韩伟红、李润恒、黄九鸣、安伦、刘为华、匡晓云、杨祎巍、刘源源、孙建国、刘涛。

网络空间安全仿真 资源管理库技术架构

1 范围

本文件规定了网络空间安全仿真资源管理库的技术架构，包括资源应用管理、安全性管理、资源库管理功能。

本文件适用于相关方对网络空间安全仿真资源进行管理。

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 25069 信息安全技术 术语

3 术语和定义

GB/T 25069-2022界定的以及下列术语和定义适用于本文件。

3.1

资源 resource

网络空间安全仿真试验进行中可使用的所有资产、能力等，可以是软件、硬件、系统、平台环境等。

3.2

样本库 sample database

用于靶标和场景构建的数据资源，包括网络流量、日志、静态文件和恶意软件等。

4 缩略语

下列缩略语适用于本文件。

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）

CPU：中央处理器（Central Processing Unit）

CVE：公共网络安全漏洞库（Common Vulnerabilities & Exposures）

DDoS：分布式拒绝服务攻击（Distributed denial of service attack）

IoT：物联网（Internet of Things）

NVD：美国国家信息安全漏洞库（National Vulnerability Database）

OSVDB：开源漏洞数据库（Open Source Vulnerability Database）

SCAP：安全内容自动化协议（Security Content Automation Protocol）
WLAN：无线局域网（Wireless Local Area Network）

5 网络空间安全仿真资源管理库概述

5.1 网络空间安全仿真资源

网络空间安全仿真资源涵盖在网络空间安全仿真试验进行中可使用的所有资产、能力等，包括靶标资源、工具资源、样本资源、知识资源、安全防护设备资源。附录A提供了网络空间安全仿真资源分类描述。

5.2 网络空间安全仿真库技术架构

本文件提出的管理技术架构对网络空间安全仿真平台中接入的相关资源管理进行规范，主要从资源应用管理、安全性管理和资源库管理功能三个方面保障安全性和可扩展性。网络空间安全仿真资源管理库技术架构见图1。

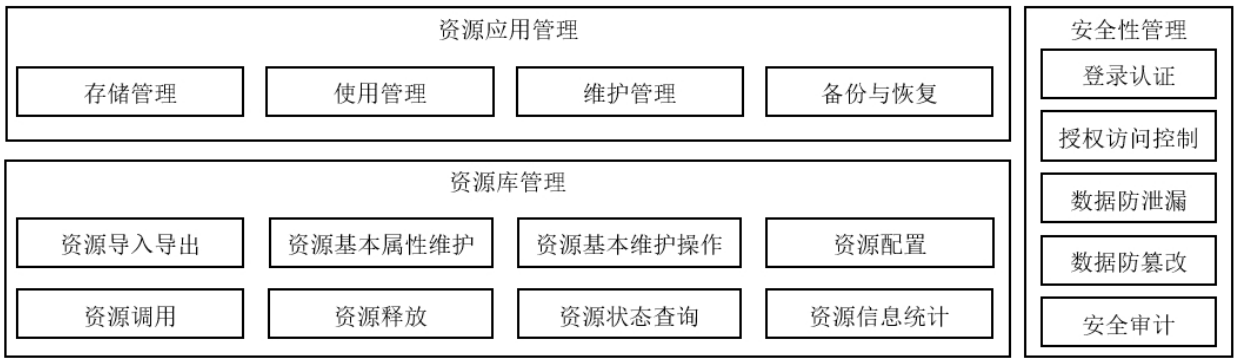

图1 网络空间安全仿真资源管理库技术架构

6 资源应用管理

6.1 概述

在资源的整体应用周期内根据资源使用的方式进行规范化管理，重点针对资源应用的四个环节即存储管理、使用管理、维护管理、备份与恢复管理提出规范要求。

6.2 存储管理

存储管理要求包括：

a) 应提供结构化与非结构化两种基础存储服务，并提供常用的调用接口；
b) 应基于私有云技术提供动态扩容、弹性扩展的存储能力；
c) 应按照本文件附录A的安全仿真资源分类示例，合理分配存储方式对资源进行分类存储；
d) 应对敏感内容提供硬件加速的加密存储能力。

6.3 使用管理

6.3.1 角色管理

应将安全仿真资源的相关方划分角色，至少包含资源创建者、资源管理者、资源审核员、资源维护员、普通用户、权限审计员等六类角色，各角色管理权限如下：

a) 资源创建者，拥有创建、提交、编辑、删除初始资源的权限；
b) 资源管理者，拥有负责安全仿真资源的构建、归集、调度、安全等权限；
c) 资源审核员，拥有审查看资源、审核资源、对资源进行提取以检测有效性的权限；
d) 资源维护员，拥有将资源上线、下线、更新等操作的权限；
e) 普通用户，拥有在安全仿真业务中使用资源的权限；
f) 权限审计员，拥有对各个角色权限边界的审核与纠偏的权限。

6.3.2 业务管理

安全仿真资源在业务过程中分为以下状态进行管理：

a) 被调用（占用）：主要指独占性的硬件类资源，如带宽资源、存储资源、计算资源等；
b) 被改变状态：主要指硬件运行状态、软件运行状态、数据处理状态等的改变；
c) 被改变组合方式：主要指在不同仿真场景使用过程中，各类安全仿真资源被快速组合，形成符合业务要求的场景与环境；
d) 被释放或删除：主要指软硬件资源的释放与数据资源的删除；
e) 被复制克隆：模板类资源在使用过程中以实例化方式运行，通过复制克隆，服务于安全仿真业务；
f) 被生成构建：脚本类资源在使用过程中，按预定配置实时生成构建；
g) 被复原：资源还原到使用前的基本状态。

6.3.3 资源管控

对资源使用的数量、位置、存储容量、网络带宽、计算能力、进程并发数、用户并发数进行管控，本项要求包括：

a) 资源数量：对软硬件资源与数据规模的量级进行限制；
b) 资源位置：对安全仿真资源使用的位置进行限制；
c) 存储容量：对安全仿真资源运行时的存储容量进行控制；
d) 网络带宽：对安全仿真资源运行时所需的带宽资源进行限制；
e) 计算能力：配置安全仿真资源的CPU参数；
f) 进程并发数：控制资源运行并发能力；
g) 用户并发数：对安全仿真资源所支撑的用户并发数进行管控。

6.3.4 审计管理

根据安全仿真资源管理库的审计角色定义，对其他角色所行使的权限边界与操作活动进行合法性审查，并确保审计数据的完整性与审计行为的规范性。

6.4 维护管理

维护管理包含资源的维护、更新、删除与销毁，本项要求包括：

a) 维护者的用户角色应是管理员；
b) 应对资源的维护操作进行全流程审计；

c） 安全仿真资源的更新支持离线更新与在线实时更新两种模式，均应通过堡垒主机，实现身份认证，实现安全管控；
d） 安全仿真资源的删除与销毁操作，应先做删除标记，从安全仿真资源管理库予以移除，经过设定时间后，再实现物理删除。

6.5 备份与恢复管理

备份与恢复管理要求包括：
a） 应对重要内容提供存储备份功能；
b） 应对资源管理库备份对象、备份介质、备份时间、备份数据保存时间和备份方式等指定备份策略；
c） 可基于资源类型、应用类型与数据类型进行自定义，根据系统级别的不同部署本地灾备与异地灾备；
d） 资源运行出现故障后，应利用备份与恢复机制实现对备份资源的还原；
e） 在还原的基础上利用日志进行资源恢复，重新建立完整的资源并继续运行。

7 安全性管理

7.1 登录认证

登录认证要求包括：
a） 所有使用仿真资源的用户均应登录认证身份；
b） 身份标识应具有唯一性，口令等身份鉴别信息应有复杂度要求并定期更换；
c） 应启用登录连接超时自动退出功能，并启用登录失败处理功能，可采取结束会话、限制非法登录次数等措施；
d） 用户身份鉴别信息丢失或失效时，应采用技术措施确保鉴别信息重置过程的安全；
e） 应支持账户口令强度配置。

7.2 授权访问控制

授权访问控制要求包括：
a） 应对访问仿真资源的用户进行授权；
b） 每个授权用户有一组安全域特性，可决定授权角色和可用权限、可用存储空间限额、可用系统资源（共享缓存、数据读写容量、CPU使用等）等安全属性；
c） 应防止授权用户无控制的使用资源管理库服务器处理器、共享缓存、资源存储介质等服务器资源，限制每个管理员及授权用户的并行会话数等功能；
d） 应建立并应用访问控制策略，对不同角色及访问行为分配相应的读取、写入等资源访问权限。

7.3 数据防泄漏

数据防泄漏要求包括：
a） 应根据资源重要程度对重要的数据和文件进行加密；
b） 应能够对进出数据进行识别，拦截非授权或异常数据，取证数据泄露行为；
c） 对传输中的数据进行泄露防护和审计，尤其是对非结构化数据的传输和外发；
d） 应根据需要采取不同的数据销毁策略和技术手段，实现对数据的有效销毁，防止因对存储介质中的数据内容进行恶意恢复而导致的数据泄漏。

7.4 数据防篡改

数据防篡改要求包括：

a) 应采用技术措施对数据存储设施进行安全防护，防止对存储数据的篡改或污染；
b) 应建立安全的加密网络隧道或其他安全措施，保障数据在传输过程中的机密性、完整性等；
c) 应对数据完整性进行校验。

7.5 安全审计

安全审计要求包括：

a) 应建立独立的安全审计系统；
b) 应对与资源安全相关的应用系统事件生成审计日志，包括用户登录和注销、用户访问应用系统功能、用户管理应用系统、应用系统出现系统资源超负荷或服务瘫痪等异常、应用系统攻击等；
c) 应对与资源安全相关的操作事件生成审计日志，包括资源的增加、删除、修改，新建、删除数据库或数据表等；
d) 应设置专门用于存储系统审计数据的安全审计库，审计日志应存储于掉电非易失性存储介质中。

8 资源库管理

8.1 资源导入导出

应提供各类资源通过规范接口导入管理库，以及从管理库导出的功能。

8.2 资源基本属性维护

应提供对资源的ID、名称、规格型号、技术参数等属性进行维护的操作接口。

8.3 资源基本维护操作

应提供针对资源进行新增、删除、修改、更新升级、权限管控等基本维护的操作接口。

8.4 资源配置

应提供对各类资源的网络拓扑、网络参数、功能、性能、安全性、快照、模板化等多方面的配置功能。

8.5 资源调用

应针对不同类型的资源，对调用方式进行统一封装，并实现独占式调用与共享式调用、本地调用与远程调用、实例化调用等多种模式的功能接口。资源被调用后，应将使用状态置为使用状态。

8.6 资源释放

应提供资源使用完毕后的资源释放接口。资源被释放后，应将使用状态置为释放状态。

8.7 资源状态查询

宜提供某一或某批资源使用状态、运行状态、计算/网络/存储性能状态、安全状态等数据的查询功能。

8.8 资源信息统计

宜提供某一或某批资源的储备数量、使用率、增长率等信息统计接口。

附 录 A
（资料性）
网络空间安全仿真资源分类示例

A.1 元数据描述

资源元数据是指对各类资源特征进行描述定义，形成统一规范的资源描述框架，方便服务接口的拓展，充分发挥网络空间安全仿真资源的使用效能。资源的元数据描述至少包含以下字段：

资源标识号（ID)：资源唯一标识编号，建议用通用唯一识别码（UUID）保证全局唯一性。

资源大类(Type)：定义资源的主要类型，如工具资源、知识库资源、样本库资源、安全防护设备资源等。

资源小类（Subtype）：定义资源的附加类型，如样本库资源里的流量样本、文件样本、数据样本。

资源中文名称（Chinese Name）：资源名称的中文表述。

资源英文名称（English Name）：资源名称的英文表述。

资源规格型号（specification & model）：资源的规格型号。

资源技术参数（Technology Parameters）：资源规格型号之外的主要技术参数。

资源IP（IP Address）：资源被分配的IP地址。

资源服务信息（Service Info）：资源可提供的服务类型信息。

资源状态（Status）：资源可用性、安全性等属性的状态。

资源备注信息（Memo）：资源的其他附属信息。

A.2 靶标

靶标资源是指网络空间安全仿真平台中用来模拟的目标，从资源形态上可以分为虚拟机靶标、容器靶标和实物靶标；从靶标的作用上可以分为基础靶标、漏洞靶标和应用靶标。在网络空间安全仿真平台中，靶标资源需要保存的信息包括靶标基本信息，靶标形态分类，靶标应用分类，靶标操作系统信息，靶标安装应用信息，靶标漏洞信息。

A.2.1 按照资源形态分类

按照资源形态分类，网络空间安全靶标资源分为以下三类。

a) 虚拟机靶标

虚拟机靶标通过虚拟化技术实现目标的模拟，展现形式为对硬件、操作系统和软件的集成式模拟，虚拟机靶标资源一般以镜像的方式存储，虚拟机的硬盘信息存储在镜像中，虚拟机运行时通过加载镜像的方式进行。

b) 容器靶标

容器靶标通过容器技术实现目标的模拟，目前流行的容器技术是Docker。Docker容器靶标一般以docker镜像或者Dockerfile方式存储。

c) 实物靶标

实物靶标一般用于模拟难以进行虚拟化或者对性能要求比较高的目标,通常是物理器件或设备的形式。

A.2.2 按照资源应用分类

按照资源应用分类，网络空间安全靶标资源分为以下三类。

a）基础靶标

基础靶标是指基础的设备、硬件、操作系统以及必要的驱动信息，或者某个版本的通用框架和中间件，用户可通过在基础靶标上增加其它资源以构建场景。

b）漏洞靶标

漏洞靶标是指专门针对某个或某些漏洞制作的靶标,用于在网络空间安全仿真平台中复现漏洞进行攻防测试和演练竞赛等。

c）应用靶标

应用靶标是指针对特定的业务系统的靶标，用于复现具体真实的业务场景。

A.3 工具集

网络空间安全仿真平台资源管理库工具资源包括信息采集类工具、合规检查类工具、测评测试类工具、网络攻击类工具、安全防护类工具等。除现有工具外，应预留工具扩展接口，根据工具库接口可自主添加新的工具。

A.3.1 信息采集类工具集

信息采集类工具集主要包括fierce工具、dnsdist6、dnsmap等。采集的信息包括域名信息、注册人信息、服务器的入侵检测系统/入侵防御系统信息、主机的操作系统信息、目标主机开启的端口、目标主机上运行的服务软件采用的数据库类型等内容。

A.3.2 合规检查类工具集

当前网络下使用的合规检查类工具集主要有以下两种：

交换机端口安全策略合规检查工具集，对接入层交换机在端口安全策略配置方面进行检测的方法，以保障交换机端口安全策略配置合规为核心，搭建全面检测交换机端口安全策略合规平台，实现对所有接入层交换机端口安全策略进行监控。

无线局域网安全检查类工具集，针对WLAN业务系统安全配置和安全漏洞检查的专业安全系统。WLAN安全检查工具集在全面识别传统网元设备安全脆弱性的基础上,增加了对WLAN系统专有协议、专有设备、专有应用的漏洞检测和合规检查。

A.3.3 测评测试类工具集

测评测试类工具包括安全功能验证、安全性验证、安全能力测评工具，包括风险评估工具、移动APP测试、硬件安全性检测、软件安全性检测、APP检测、密码测评、等保测评、源代码审计、自动化漏洞挖掘、自动化渗透测试、网络安全意识与技能测评等工具，可以是单个工具或多个工具组成的集合工具流。

A.3.4 网络攻击类工具集

网络攻击工具包括能够扰乱计算机系统正常工作导致系统拒绝服务,破坏系统数据或在系统内造成安全隐患的口令、程序或软件，包括网络扫描工具、电子邮件炸弹、蠕虫病毒、计算机病毒、特洛伊木马、逻辑炸弹、勒索病毒、后门口令程序、DDoS工具（loic、xoic等）、开源通用工具集（信息收集、扫描、爆破、代理、嗅探）、等。

A.3.5 安全防护类工具集

安全防护类工具包括：网络资产测绘工具、终端安全工具、网络安全工具、云安全工具、数据安全工具、逆向工程分析工具、数据库安全检测工具、安全基线检查（配置检查）工具、应急响应工具、工

控系统安全工具、IoT安全工具、fuzz测试工具集（bunny、spike等）、网络访问匿名化、蜜罐与蜜网等。

A.4 样本

A.4.1 流量样本

流量样本主要包括：

a）常见的互联网各种业务应用和协议仿真，混合不同协议的应用流量场景；

b）真实的互联网上针对漏洞的攻击、病毒、恶意软件、DDoS、BOTNET的仿真；

c）各种黑客的行为仿真、钓鱼网站、垃圾邮件、绕过安全对策的逃避战术等；

d）生成包含无效数据和异常数据的Fuzzing流量；

e）各种受到监控和追踪的目标数据。

A.4.2 文件样本

文件样本是指各类操作系统文件类数据资源，包括恶意程序静态文件。

A.5 知识

A.5.1 基础知识库

基础知识库存在于网络渗透测试攻击子系统中，以视频、课件、教材、BLOG等形式呈现。主要包括信息安全法律法规、IoT安全知识、逆向安全知识、Web安全知识、主机安全知识、数据库安全知识、网络安全攻防知识、溢出类安全知识、密码学知识、网络安全基础知识、社会工程学知识、等级保护知识、风险评估知识、安全加固知识、渗透测试知识、安全运维知识、信息安全管理知识等。

A.5.2 漏洞

漏洞库资源包含国内外主要漏洞库、安全厂商整合和自主挖掘未公开的关于应用、系统、数据库网络设备的漏洞。国内漏洞库主要包括：CNNVD、CNVD、SCAP中文社区、Sebug漏洞库等。国外漏洞库主要包括CVE、NVD、Security、Focus、Secunia、OSVDB、Metasploit、PacketStorm、Security、Reason等。

A.5.3 威胁情报

威胁情报数据包括安全设备拦截、后台安全信息和事件管理等安全分析系统的分析及业务风险控制系统的发现，以及来自第三方提供或共享的多源情报，包括漏洞情报。

A.5.4 模型

由仿真开发人员开发的仿真模型，是仿真业务的基本单元，各个模型有不同的环境需求。包括神经网络模型、决策树模型、关联规则模型、支持向量机模型、朴素贝叶斯模型、混合高斯预测模型、以及线性或逻辑回归算法、排序、抽样等。

A.5.5 课件

在网络空间安全仿真平台的教学环节中，课件库提供基于课程材料与实验环境的网络空间安全仿真平台教学，覆盖常见网络安全通识、网络攻击、网络防御、网络检测等内容。

A.5.6 竞赛试题

网络空间安全仿真平台竞赛试题主要包含信息安全基础、Web安全、PKI、密码学、入侵检测系统、安全风险评估、代码审计、溢出、数字水印、数据库安全、中间件加固、渗透测试、网络嗅探、端口扫描、病毒防范、网络攻防实战等。

A.5.7 攻防场景构件

攻防场景库内置的由各类靶标和虚拟网络组成的攻防场景构件。可根据需要用来进行组合、裁剪和加工，以构建满足渗透测试、安全加固、应急响应、系统安全性测试等实验或测试的特定场景。

A.5.8 其它知识

其它不属于上述分类的知识，如小技巧和经验等非标准形式的知识积累

A.6 安全防护设备

A.6.1 终端安全设备

针对终端提供防护功能的安全设备，包括移动终端安全系统、APP加固平台、主机检测与审计、安全操作系统等。

A.6.2 网络安全设备

部署在网络上、基于网络安全流量处理提供安全防护功能的安全设备，包括防火墙、入侵检测与防御、网络隔离和单向导入、防病毒网关、上网行为管理、网络安全审计、堡垒机、VPN、抗拒绝服务攻击、网络准入设备、工控安全产品等。

A.6.3 应用安全设备

针对特定应用类型提供多方防护功能的安全设备，包括Web应用防火墙、Web应用安全扫描、网页防篡改、邮件安全系统。

A.6.4 数据安全设备

保障数据安全的各种安全设备，包括数据库审计与防护、安全数据库、数据泄露防护、文件管理与加密、数据备份与恢复、数据脱敏设备等。

A.6.5 其他安全设备

拟态防御、可信计算、量子通信、区块链安全、蜜罐蜜网等安全设备。