ICS 35.240.01

CCS L 60

T/CSAC

团　　体　　标　　准

T/CSAC XXX—XXXX

网络靶场 资源描述要求

Cyber range- Request to resource description

（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），湖南星汉数智科技有限公司，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，软极网络技术（北京）有限公司，四川亿览态势科技有限公司，电子科技大学，北京理工大学，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，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，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，博智安全科技股份有限公司。

本文件主要起草人：贾焰，胡宁，郑涛，李树栋，韩伟红，顾钊铨，安伦，李润恒，蔡晶晶，陈俊，邱欣逸，周可，陶莎，黄九鸣，谢玮，孟楠，罗蕾，危胜军，杨彦召，薛信钊，汪向阳，王帅，金华敏，杨祎巍，赵焕宇，燕玮，徐天妮，邱勤，陈璐，李雪莹，王绍杰，傅涛，郑轶，王龑，匡晓云，陶冶，张凯，李炜。

引　　言

网络空间对抗形势日趋严峻，网络攻防已成为各国网络空间对抗的主要内容。世界各国均高度重视网络靶场建设，将其作为支撑网络空间安全技术验证、网络武器试验、攻防演练和网络风险评估的重要手段。网络靶场用于网络攻防演练、人才培养、网络安全技术及网络新技术测评等，支持提升网络和信息系统的稳定性、安全性和性能，已成为各国开展网络空间安全领域的研究、学习、测试、验证、演练等所需的核心基础设施。

随着很多领域、应用场景都开始建设网络靶场，网络靶场中包含越来越多种类的资源。不同靶场对于资源的描述、传递方式有各自不同的标准，这为网络靶场之间的资源交互带来了极大的不便。为了解决这种不便，因此有必要对网络靶场中的各类资源的描述作出统一的要求，规定网络靶场资源如何描述其组成，促进网络靶场的互联互通，进一步指导和促进各领域网络靶场的建设和应用。

网络靶场 资源描述要求

1 范围

本文件规定了网络靶场中的原子资源、组合资源等 2 大类资源的基本属性、访问属性、操作方法等方面的描述方式。

本文件适用于指导网络靶场中所有资源的统一描述方式。

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。

2019-0981T-YD 网络安全空间仿真 术语

3 术语和定义

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

资源 resource

在网络靶场试验过程中可使用的所有资产、能力等对象。

3.3

原子资源 atomic resource

网络靶场中最基本、不可分割的资源。

3.4

组合资源 combine resource

网络靶场中若干原子资源组合形成的资源。

3.5

数据类型资源 data resource

原子资源中的一种，网络靶场中所有的数据。

4 缩略语

下列缩略语适用于本文件。

IP　　互联网协议（Internet Protocol）

5 概述

网络靶场资源是在网络靶场中的可使用的所有资产对象。为了准确描述网络靶场资源，本文件规定了网络靶场资源的基本原子分类，并且所有资源均可描述为由五大原子类资源构成的组合资源。

根据存在形式、使用方式、构成介质等标准将网络靶场资源基本组成分类成以下五大基本原子资源，实体设备类资源、虚拟设备类资源、系统软件类资源、应用软件类资源、数据类资源。如下图 1：

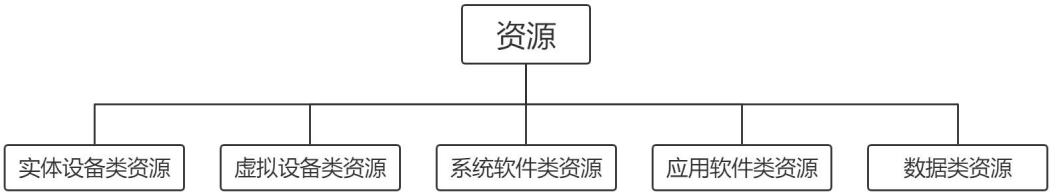


图 1 资源分类图

a）实体设备类资源

网络靶场中真实存在的设备，包含：实体服务器、虚实互联交换机、实体防火墙等

b）虚拟设备类资源

网络靶场中虚拟化出来的设备，包括：虚拟交换机、虚拟防火墙、KVM 虚拟化等

c）系统软件类资源

网络靶场中的系统软件，包括：Linux 操作系统、Windows 操作系统、渗透操作系统等

d）应用软件类资源

网络靶场中的应用软件，包括：web 服务、渗透工具、防御工具等

e）数据类资源

网络靶场中的所有数据信息，包括：公网域名、公网 IP 等

利用面向对象的特性，提出了组合资源这一概念。组合资源是网络靶场资源的最常见资源类型，是由若干原子资源以单层或者多层的结构形式组合形成，以实现各种相对复杂的功能需求。

组合资源的组合形式有如下几种：

a） 单原子组合：组合资源由多个单种原子资源组合而成，包括：交换机集群、虚拟机集群等

b） 多原子组合：组合资源由多个不同种类原子资源单层或者多层构建组合而成。包括：试验目标网络、靶标等

6 网络靶场原子资源的描述要求

6.1 原子资源描述模型

结合原子资源自身的基本特性，建立原子资源模型。原子资源包含基本属性、访问属性以及操作方法，如下图 2 所示。

a) 基本属性是原子资源反映其基本类型、特性、功能等内容的数值，包括：设备类型、系统类型、应用类型、品牌、型号、文件名、数据结构、数据存储方式、功能描述、备注说明等。
b) 访问属性是反映原子资源的复用能力的权限，包括：可共享、可读、可写、可运行等。
c) 操作方法是原子资源给出的指导性操作指南，包括：操作名称、使能对象、操作流程、操作备注等。

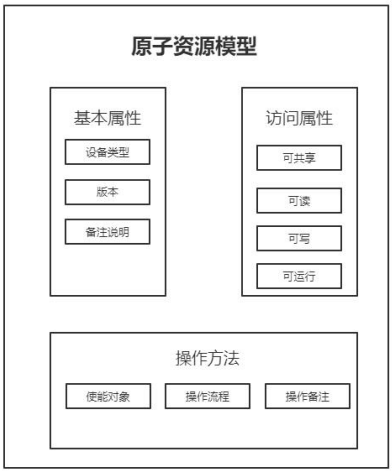


图 2 原子资源模型图

6.2 原子资源的基本属性

每种基本原子资源包含了各自的基本属性，其基本属性表现出该原子资源的类型、性能、状态等等特性。基本属性的数据类型主要为字符、数字等。

不同的原子资源既有其独特的基本属性，比如实体设备的外形尺寸就是实体设备类资源的独有基本属性；不同的原子资源也包含与其他部分原子资源相同的基本属性，比如虚拟设备、系统软件、应用软件都包含版本这个基本属性。五种原子资源的常用基本属性如下表 1 所示：

表 1 原子资源基本属性表

原子类型	实体设备	虚拟设备	系统软件	应用软件	数据
基本属性	设备类型	设备类型	系统类型	应用类型	数据结构
	品牌	版本	版本	版本	存储方式
	型号	虚拟化平台	名称	名称	数据内容
	外形尺寸	备注说明	存储	适配系统	存储位置
	管理方式		备注说明	备注说明	操作方式
	备注说明				备注说明

6.3 原子资源的访问属性

原子资源的属性除了基本属性外，还包含一类特殊的属性，称为访问属性。访问属性就是对该原子资源的复用方式的说明属性，表名该原子资源是否可以被复用以及如何被复用。访问属性的属性值固定为布尔型。五大原子资源的常用访问属性如下表 2：

表 2 原子资源访问属性表

原子类型	实体设备	虚拟设备	系统软件	应用软件	数据
访问属性	可迁移	可复制	可共享	可共享	可共享
	可共享	可共享	可读	可读	可读
	可读	可读	可写	可写	可写
	可写	可写	可运行	可运行	可运行
	可运行	可运行			

6.4 原子资源的操作方法

原子资源除了包含基本属性、访问属性之外，还拥有各自的操作方法。操作方法内详细说明了该原子资源的使用流程等。操作方法中包括操作名称、使能对象、操作流程、操作参数、操作备注等。各个原子资源的操作方法的几大内容均为可选内容，有相关内容即描述，没有相关内容可不描述，如下表 3：

表 3 原子资源操作方法表

原子类型	实体设备	虚拟设备	系统软件	应用软件	数据
操作方法	操作名称	操作名称	操作名称	操作名称	操作名称
	使能对象	使能对象	使能对象	使能对象	使能对象
	操作流程	操作流程	操作流程	操作流程	操作流程
	操作参数	操作参数	操作参数	操作参数	操作参数
	操作备注	操作备注	操作备注	操作备注	操作备注

7 网络靶场组合资源的描述要求

7.1 组合资源模型

组合资源是由多个原子资源以单层或者多层结构组合形成。组合资源内容与原子资源内容的结构相同，同样包含基本属性、访问属性、操作方法。模型图如下图 3：

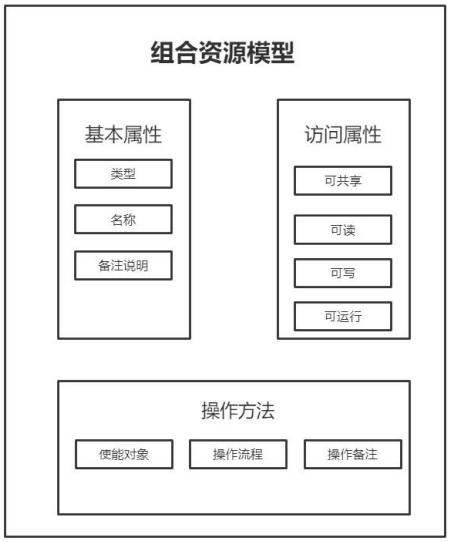


图 3 组合资源模型图

7.2 组合资源的基本属性

组合资源的基本属性与原子资源的基本属性相同，其内容部分由以下两部分组成。

a) 继承来自子资源的基本属性，例如：交换机集群的设备类型、外形尺寸等

b) 组合资源自身独有的基本属性，例如：靶标的 IP 等

7.3 组合资源的访问属性

组合资源的访问属性是对该组合资源复用的权限说明属性，访问属性的属性值固定为布尔型。组合资源的复用权限与其组成资源的复用权限并不相等，以靶标组合资源及其子资源访问属性对比为例。如下表 4：

表 4 组合以及子资源访问属性对比

	靶标组合资源	web 服务子资源
可共享	false	true
可读	true	true
可写	false	false
可运行	true	true

7.4 组合资源的操作方法

组合资源模型的操作方法内容格式与原子资源的基本一致，如下表 5 所示。

表 5 操作方法对比表

原子类型	原子资源	组合资源
操作方法	操作名称	操作名称
	使能对象	使能对象
	操作流程	操作流程
	操作参数	操作参数
	操作备注	操作备注

组合资源的操作方法主要分为两种：

a) 继承部分来自子资源的操作方法，部分子资源操作方法在组合资源中仍然可行，组合资源即可添加这一操作方法。

b) 组合资源自身产生的新操作方法，在其子资源中不存在该方法，仅当前组合资源才具备的可操作性。

附 录 A
原子资源实例

资源类型	原子资源实例	资源描述示例

实体设备类资源	交换机资源	{
		“基本属性”：
		{
		“设备类型”: “实体网络设备”,
		“品牌”: “H3C”,
		“型号”: “s6300”,
		“外形尺寸”: “440X160X43.6mm”,
		“功能描述”: “H3C S6300 系列交换机通过创新的体系架构大幅简化了数据中心网络结构；在提供高密 10GE/40GE 线速转发端口基础之上，还支持灵活的模块化可编程能力及丰富的数据中心特性。”,
		“备注说明”: “接入交换机”
		}
		“访问属性”：
		{
		“可共享”: true，
		“可读”: true，
		“可写”: ture，
		}
		“操作方法”：
		{
		“操作名称”： “安装交换机”
		“使能对象”：“用户”
		“操作流程”： “连接保护地线，安装风扇模块，安装电源模块，连接电源线”
		“操作参数”： “–”
		“操作备注”： “–”
		}
		}

虚拟设备类资	虚拟防火墙资源	{ “基本属性”： { “设备类型”: “虚拟化网络安全设备”, “版本”: “vFW1000”, “支持的虚拟化平台”: “VMware ESXi\Linux KVM\H3C CAS”,

源		“虚拟化文件格式”: “ISO”,
		“管理方式”: “Console，Telnet，SSH，HTTP，SNMPv3”,
		“功能描述”: “提供防火墙过滤，NAT 应用，安全管理，安全认证，VPN，SDN 等功能”
		}
		“访问属性”：
		{
		“可共享”: true，
		“可读”: true，
		“可写”: false，
		}
		“操作方法”：
		{
		“操作名称”： “安装防火墙”
		“使能对象”：“用户”
		“操作流程”： “连接保护地线，连接电源线，连接防火墙到配置终端，通电”
		“操作参数”： “–”
		“操作备注”： “–”
		}
		}

系统软件类资源	Windows 操作系统资源	{
		“基本属性”：
		{
		“系统类型”: “windows”,
		“版本”: “Windows 10 (Multiple Editions) Insider Preview 14295 (x64)”,
		“文件名”:
		“cn_windows_10_multiple_editions_insider_preview_14295_x64_dvd_8475180.iso”,硬盘空间 16GB(32 位)或 32GB(64 位)”,
		“文件大小”: “3.99GB”
		}
		“访问属性”：
		{
		“可共享”: true，
		“可读”: true，
		“可写”: false，
		}
		“操作方法”：
		{
		“操作名称”： “安装系统”
		“使能对象”：“用户”
		“操作流程”： “制作 PE 启动 U 盘，进入 boot 快速启动菜单页面，启动 PE 安装”
		“操作参数”： “–”

		“操作备注”： “–” } }

应用软件类资源	nginx服务应用资源	{
		“基本属性”：
		{
		“应用类型”: “应用服务”,
		“文件名”: “nginx-1.23.1.tar.gz”,
		“应用名称”: “nginx”,
		“版本”: “1.23.1”,
		“文件格式”: “tar.gz”,
		“文件大小”: “1.05 MB”,
		“适配的操作系统”: “Windows，Linux”
		}
		“访问属性”：
		{
		“可共享”: true，
		“可读”: true，
		“可写”: false，
		}
		“操作方法”：
		{
		“操作名称”： “安装软件”
		“使能对象”：“用户”
		“操作流程”： “安装依赖包，下载解压安装安装包，安装nginx，启动nginx服务，配置nginx.conf，重启nginx”
		“操作参数”： “–”
		“操作备注”： “–”
		}
		}

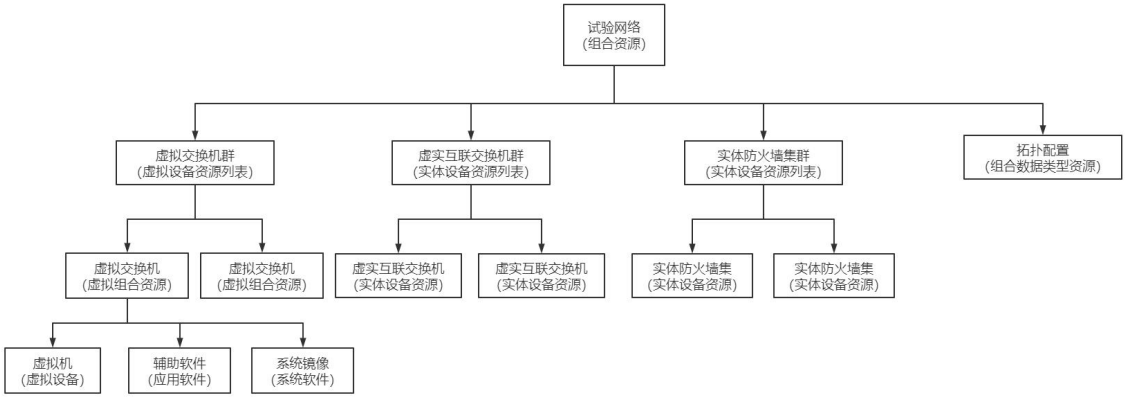
数据类资源	拓扑日志数据资源	{
		“基本属性”：
		{
		“数据结构”: “log”,
		“数据内容描述”: “用于记录网络拓扑搭建的过程信息”,
		“数据来源”: “目标网络”,
		“存储位置”: “log/”,
		“操作方式”: “可读”,
		}
		“访问属性”：
		{
		“可共享”: false，
		“可读”: true，

		“可写”: false，
		}
		“操作方法”：
		{
		“操作名称”： “读取日志”
		“使能对象”：“用户”
		“操作流程”： “远程连接到系统服务器，进入日志服务器，查询日志位置，拷贝日志”
		“操作参数”： “–”
		“操作备注”： “–”
		}
		}

附 录 B
组合资源实例

下面以试验网络为例，进行组合资源的说明，展示其组成图及资源描述示例。

一个试验网络由虚拟交换机群、虚实互联交换机群、实体防火墙集群、拓扑配置四个子组合资源组合而形成。其中虚拟交换机群、虚实互联交换机群又是由各自的单体虚拟交换机、单体虚实互联交换机堆叠组合形成的列表组合资源。每台可使用的虚拟交换机又包括三种基本原子类资源：虚拟设备、应用软件、系统软件。



组合资源实例	资源描述示例

试验网络	{
	“基本属性”：
	{
	“交换机品牌”: “H3C”,
	“交换机型号”: “s6300”,
	“防火墙版本”: “vFW1000”
	“网段”: “10.6.2.0-10.6.2.255”,
	“IP 白名单”: “10.122.122.*”
	“发布时间”: “2016-03-30”,
	“功能描述”: “目标网络的试验环境”,
	“备注说明”: “无”
	}
	“访问属性”：
	{
	“可共享”: false，
	“可读”: true，
	“可写”: false，
	}
	“操作方法”：
	{

	“操作名称”： “添加虚拟交换机” “使能对象”：“用户” “操作流程”： “创建新的虚拟交换机，连接到虚拟交换机集群中” “操作参数”： “–” “操作备注”： “–” } }