

# 《网络靶场 平台能力分级指南》 编制说明

网络靶场平台能力分级指南标准起草组

2023年3月

## 1. 标准立项的背景、目的和意义

目前国内外尚未对网络靶场的能力进行分级与评估，行业缺少统一的分级标准和描述规范描述。形成《网络靶场能力分级指南》目的在于对不同领域和不同行业网络靶场的使用场景进行细化分类，从而形成网络靶场能力描述和分级规范，快速实现网络靶场间的交互。

## 2. 标准范围

随着很多领域、应用场景都开始建设网络靶场，不同网络靶场具备的功能特点各异。因此，有必要定义网络靶场中黄方、白方、绿方、红方、蓝方五方角色应具备的主要功能及能力进行分级，包括黄方系统的导调指挥能力、白方系统的目标网络仿真构建与互联接入能力、绿方系统的攻击检测与态势评估能力、红方系统的攻击工具管理及组装能力、蓝方系统的防御工具管理及协同运行能力。通过制定本文件，为网络靶场的能力分级提供规范，进一步指导和促进各领域网络靶场的建设和应用。

## 3. 工作简况

《网络靶场 能力分级指南》于2023年2月提出立项申请。

本标准的牵头起草单位包括：鹏城实验室、广州大学、中国电信股份有限公司。

本标准的参与起草单位包括：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)，中国信息通信研究院、北京永信至诚科技股份有限公司、电子科技大学、北京理工大学、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、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、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、博智安全科技股份有限公司、中电长城网际系统应用有限公司。

本标准的制定过程包括以下几个阶段：

形成征求意见稿阶段（2023年1月-2023年2月）。

2023年1月启动该标准的编制工作。在标准制定过程中，鹏城实验室牵头组织各起草单位对《网络靶场 平台能力分级指南》进行了分析和研究，标准编制组于2023年1月底完成标准草案。

2023年2月24日在中国网络空间安全协会组内讨论会上提出立项申请并通过立项。

#### 4. 标准编制原则和确定标准主要内容的依据

本标准在编制过程中注意到了RFC 8200中IPv6协议本身协议规定的一致性，参照相关流量整形技术的标准要求，设计承载流量整形机制的协议并提出技术和安全要求，做到技术先进合理，切实可行。

标准文本按GB/T 1.1-2020《标准化工作导则第1部分：标准的结构和编写》的要求编写。

本标准完善用IP协议来适配同步流量整形机制，能够解决互联网由于复杂的网络结构和多样的通信需求而产生的多协议兼容和数据互联互通困难的问题。针对IP协议承载确定性网络技术协议的适配完善了协议优化设计，将确定性保障能力通过网络层技术拓展传递，解决IPv6缺乏将底层特性转换为上层应用能力的问题。

#### 5. 主要试验情况分析

本标准针对网络靶场的不同能力，对网络靶场的主要功能给出了定义以及依据主要功能提出了分级要求，有助于统一网络靶场制定标准的攻击行为检测流程。

同时，本标准在制定过程中，与院校合作研究机构、国家互联网应急协调组织、网络安全企业进行了充分的讨论，在标准中充分保证了研究机构及相关单位的专利产权，尤其是相关企业的竞争力。

6. **重大分歧意见的处理经过和依据**  
无。
7. **采用国际标准和国外先进标准情况**  
目前国际上尚无与本标准等效或等同的国际建议。
8. **替代或废止现行相关标准的建议**  
本标准为新制定标准。
9. **与现行相关法律、法规、规章及相关标准的协调性**  
本标准与现行法律、法规没有抵触。  
本标准不涉及到国家强制性标准，不存在冲突与矛盾。
10. **标准性质的建议**  
建议本标准批准后作为推荐性标准使用。
11. **贯彻国家标准的要求和措施建议**  
无。
12. **知识产权情况说明**  
本标准不涉及知识产权问题。
13. **其它应予说明的事项**  
无其他应予说明的事项。