《网络空间安全仿真 基于技战术体系的安全测评方法》

编制说明

《网络空间安全仿真 基于技战术体系的安全测评方法》

标准起草组

1. 标准立项的背景、目的和意义

网络安全评测是安全建设的基础性工作，只有在正确、全面地了解防护能力后，在安全投入、安全措施选择、安全保障体系建设等问题中做出合理的决策。

传统安全测评往往基于等保合规的理念，仅能针对网络安全产品和网络安全能力的合规性进行评估，但无法评估现有防御有效性、安全投入效能和安全能力差距等问题。基于传统安全评测的安全建设，也往往会陷入安全产品的堆砌、重复建设，投入大但防护能力不足的怪圈。

伴随攻击技术变化，网络安全防护能力的持续提升，安全评测标准已无法有效地评估网络信息系统的防护能力。现有测评标准中对网络安全能力的要求均基于低抽象模型和单点检测方式，无法覆盖网络攻击技术和手段不断变化。此外，各个安全厂商宣称的攻击溯源、全事件检测能力，需要统一的基线进行更客观，平等的评估。

基于攻击技战术模型的安全评测利用 ATT&CK 框架作为评估“标尺”，采用白盒模拟测试方法，最大程度减轻了传统安全服务效果取决于评测人员安全能力的弊端，可帮助组织快速形成安全检测能力，提高组织针对于高级威胁检测的“广度与深度”。

但是，各安全厂商或机构仅参考攻击技战术模型，按照各自的理解去执行攻防测试或演练，战术、技术和程序是否得到合理有效的利用，是否达到整体最优很难界定，如何将攻击技战术从整体系统化的模拟出来，应用于安全评测，业界并没有统一的标准来体系化的模拟

和应用这套模型，以达到从整体上实现体系化、最优的攻防效果。

通过该标准，为组织和第三方机构开展相关安全评测提供了工作指导和参考，具有较大技术和社会价值。

2. 标准范围

本文件规定了基于攻击技战术模型，在网络空间安全仿真环境中利用模拟攻击进行安全评测的准备要求、指标要求，测试及评估方法。本文件适用于指导组织基于攻击技战术模型开展安全评测工作。

3. 工作简况

《网络空间安全仿真 基于技战术体系的安全测评方法》是中国网络空间安全协会2023年3月立项的团体标准。本标准的牵头起草单位为：鹏城实验室，参与起草单位包括：广州大学、哈尔滨工业大学(深圳)、北京升鑫网络科技有限公司、中国电信股份有限公司广东研究院。

在标准制定过程中，鹏城实验室牵头组织各起草单位对《网络空间安全仿真 基于技战术体系的安全测评方法》进行了分析和研究，并形成征求意见稿，提交会议公开征求意见。

4. 标准编制原则和确定标准主要内容的依据

本标准制定过程中以遵循国际标准、国家标准和满足国内应用为指导思想，坚持标准的实用化原则，坚持目前急需与将来进一步发展

需要相结合的原则。

本标准主要基于攻击技战术模型（ATT&CK 模型），定义了在网络靶场环境中通过模拟攻击开展安全测评的方法、要求和指标。

ATT&CK 模型是在洛马公司提出的 Kill Chain 模型的基础上，构建的一套更细粒度、更易共享的知识模型和框架。ATT&CK 是一个基于黑客攻击实战结果建立的网络攻击战术和技术的知识体系，它描述了网络攻击的行为模型，反映出整个攻击周期的各个阶段。ATT&CK 包含三个核心部分，即战术、技术和过程（TTPs），战术表示攻击者的目标，技术表示攻击者达成战术目标的方法与手段，过程显示攻击者如何执行某项技术。

在国外，从 2018 年开始，MITRE Engenuity 开始模拟真实世界的攻击手法来测试端点安全产品，主要使用当年影响比较大的某个黑客团体的技术。在国内，已有部分厂商提供了相关测评服务。上述安全测评工作都在不同程度上使用了攻击技战术模型来对产品或系统等进行评测，并且都取得了较好的效果，但是评估所需的攻击向量选取标准、评估要素和赋值规则等各不相同。目前，国内外尚没有制定过利用实际攻击评测，特别是基于攻击技战术模型安全评测的国家或者行业标准。

制定基于攻击技战术模型的安全评测相关标准，符合等保 2.0 安全区域边界-入侵防范章节，“实现对网络攻击特别是新型网络攻击行为的分析”的要求。通过该系列标准，为组织和第三方机构开展相关安全评测提供了工作指导和参考，具有较大技术和社会价值。

标准的用语、格式按照GB/T1.1-2020给出的规则起草。

5.主要试验情况分析

本标准通过制定基于攻击技战术模型的安全评测方法，符合等保2.0安全区域边界-入侵防范章节，“实现对网络攻击特别是新型网络攻击行为的分析”的要求。通过该系列标准，为组织和第三方机构开展相关安全评测提供了工作指导和参考，具有较大技术和社会价值。

同时，本标准在制定过程中，与高校、网络安全企业进行了充分的讨论，在标准中充分保证了高校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

暂无。

7.采用国际标准和国外先进标准情况

项目参考的国外安全评测类标准有：

（1）ISO/IEC 15408 Information technology — Security techniques—Evaluation criteria for IT security

（2）ISO/IEC 18045:2008 Information technology—Security techniques—Methodology for IT security evaluation

（3）ISO/IEC 27000 Information technology — Security

techniques — Information security management systems — Overview and vocabulary

（4）NIST SP 800-53 Assessing Security and Privacy Controls in Information Systems and Organizations

（5）NIST SP 800-115 Technical Guide to information security testing and assessment

暂未发现基于攻击技战术模型的安全评测对应的国际或国外标准。

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

目前，国内尚无基于攻击技战术模型的安全评测国家或行业标准，GB/T 20984-2007《信息安全技术 信息安全风险评估规范》系列标准规定了信息安全风险评估的方法和要求，但是并不涉及对网络产品和安全产品的攻防评测的相关内容。

10.标准作为强制性标准或推荐性标准的建议：

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

制定基于攻击技战术模型的安全评测相关标准，符合等保 2.0 安全区域边界-入侵防范章节，“实现对网络攻击特别是新型网络攻击行为的分析”的要求。通过该系列标准，为组织和第三方机构开展相关安全评测提供了工作指导和参考，具有较大技术和社会价值。

12. 知识产权的情况说明

无。

13. 其他应予说明的事项

无。