企业安全防御体系的智能化有效性验证方案研究

Research on Intelligent Effectiveness Verification Scheme for Enterprise Security Defense System

杨丽丽，刘　果，戚大强，张　彬，高贯银（中讯邮电咨询设计院有限公司，北京 100048）
Yang Lili，Liu Guo，Qi Daqiang，Zhang Bin，Gao Guanyin（China Information Technology Designing & Consulting Institute Co.，Ltd.，Beijing 100048，China）

摘　要：
常用的有效性验证手段大大控制了企业的安全风险，但也存在很多客观制约条件。提出了智能化有效性验证方案，首先进行可视化的二维坐标攻击面管理和积累攻击方法、技术、路径的系统知识库；然后基于攻击面和系统知识库进行“双视角”的攻击模拟模型训练，通过AI调度算法和攻击模拟模型对企业安全防御体系进行持续验证；对验证过程进行复盘、整改、调优。该方案可有效管控系统风险，快速核验系统攻击知识的信息，使验证的活动可持续。

关键词：
攻击面管理；攻击模拟；有效性验证
doi：10.12045/j.issn.1007-3043.2023.08.015
文章编号：1007-3043（2023）08-0067-04
中图分类号：TN915.08
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
Frequently-used effectiveness verification methods greatly control the security risks of enterprises，but there are also many objective constraints. It proposes an intelligent effectiveness verification scheme，and firstly it establishes a visual two-dimensional coordinate attack surface management and accumulates a systematic knowledge base of attack methods，technologies and paths. Then，based on the attack surface and system knowledge base，a "dual-perspective" attack simulation models is trained，and the enterprise security defense system is continuously verified by AI scheduling algorithm and attack simulation model. Then，the verification process is reviewed，rectified and optimized according to the verification results.This plan can effectively control system risks，quickly verify the information about system attack knowledge，and make verification activities sustainable.

Keywords：
Attack surface management；Attack simulation；Effectiveness verification

引用格式：杨丽丽，刘果，戚大强，等. 企业安全防御体系的智能化有效性验证方案研究[J]. 邮电设计技术，2023(8)：67-70.

0 前言

企业为了满足各项等保要求和自身安全风险控制，在建设完备企业安全防御体系的同时，也在持续地对其进行有效性验证，不断纵深安全防御体系，保障业务安全运行。

随着业务复杂度提升、防御工具的多样化，有效性的验证方式从基础的基线检查再到实战演练的红蓝对抗，无一例外都着眼企业安全防御的有效性。常规的安全有效性验证手段帮助企业解除了一定的安全隐患，但是也暴露了不同程度的问题。比如：基线检查奠定了企业网络信息建设的安全基础，但缺少实时、动态、自动化的验证能力；渗透测试高度依赖于渗透人员的经验，带来了有效性验证覆盖面的不确定性；实战化的红蓝对抗对企业暴露面进行全面验证，但是受限于时间、成本，验证过程很难持续，且漏洞利用的关联性随着验证活动结束容易被忽略。

从以上有效性验证手段来看，验证过程是静态的，并且带来了覆盖面不确定、活动难持续、知识遗失等问题，但红蓝对抗活动的红方攻击行为是接近真实环境的攻击形式，所以红方的攻击技术、路径、思路是本方案中建立有效性验证的原型基础。以红方视角

收稿日期：2023-06-08

的有效性验证进行全量攻击面及攻击向量的管理有利于验证过程中快速发现新的攻击面和新漏洞利用。以蓝方视角将资产的丰富性，组织的丰富性，合作伙伴纳入到扩展的攻击面管理中，通过攻击模拟模型学习新的攻击场景知识，持续地对系统暴露面进行验证，发现系统防御“死角”和评估风险严重程度。

智能化的有效性验证方案需要依靠准确的攻击面管理、全面的攻击场景知识库、自动化的调度攻击模拟模型，持续地、自动化地对企业的安全防御体系进行验证，让更多的未知变已知，已知为未知提供更多的探索样本。

1 整体方案

如图1所示，本方案是从攻防演练中红蓝双方视角出发，首先通过系统台账以及智能化的资产发现工具收集系统暴露面，进行全量的攻击面和攻击向量管理和量化评估；通过攻防演练时红方对目标渗透时的方法、技术和路径形成业务系统攻击场景知识库，情报信息积累形成通用型攻击知识库；通过自动化的调度算法，对攻击模拟模型中的不同类型的攻击模型进行调度，从信息对称和信息不对称2个维度，分别对模型进行有监督和无监督的验证训练；信息不对称的攻击模拟主要实现未知攻击面的挖掘和新型漏洞的验证和利用。信息对称的攻击模拟主要基于完全已知的系统基础建设、系统漏洞等信息进行攻击面覆盖和威胁程度的确认。针对双重视角的验证结果进行每一轮复盘，为丰富知识库和优化攻击模拟模型提供依据。

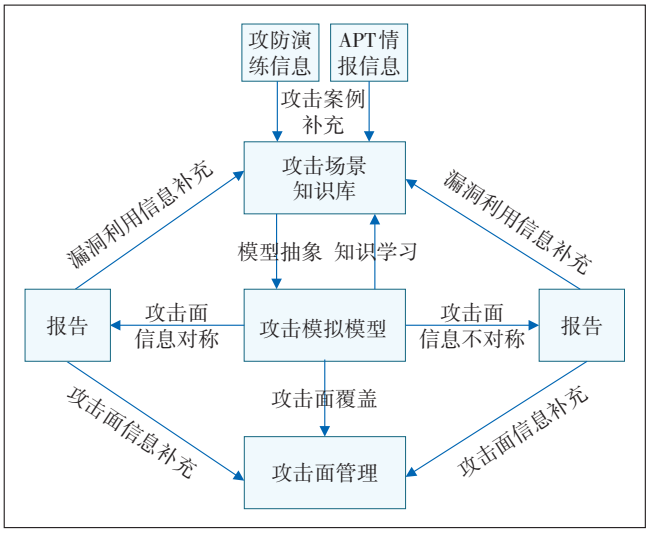

图1　整体方案示意

a）攻击面管理：通过系统台账、智能爬虫、指纹识别等技术对多类型、广泛的资产范围进行识别，基于识别的资产范围进行漏洞扫描、漏洞验证，对漏洞的真实性以及风险指数进行初步评估，再利用攻击模拟模型进行场景化的漏洞利用验证，最后形成以资产为横轴、漏洞为纵轴，风险评价指标量化的系统攻击面管理。

b）攻击场景知识库：知识库的积累来源于企业主动的有效性验证（红蓝对抗等）活动或者企业被动攻击（黑客入侵案例）事件。在红蓝对抗活动中通过红方成功提权结果进行痕迹溯源，自动识别新知识，添加进系统业务攻击知识库。另外收录一些情报组织的安全攻击事件，这些攻击模式相对固定，且具有较明显的可识别性，形成系统通用攻击知识。

c）攻击模拟模型：攻击模拟模型旨在以黑客的攻击视角验证系统防御的有效性。本模型中引入入侵和攻击模拟（Breach Attack Simulation，BAS）技术实现对真实业务目标进行攻击模拟，通过控制对目标发送payload，避免对目标的业务运行产生影响。以信息对称视角进行有监督模型训练，不对称视角进行无监督模型训练，建立各自的攻击场景剧本。

d）攻击报告及复盘：通过攻击报告展示整体系统风险评估、攻击漏洞及单漏洞利用或联合利用的路径，为用户提供修复建议，以攻击者视角帮助用户提升网络安全防护能力。同时通过对攻击报告的复盘，补充系统的幽灵资产以及新形态的攻击场景知识。

2 核心功能

2.1 攻击面管理

攻击面管理是企业资产面临的所有攻击向量的总和，攻击向量是攻击者对系统进行的攻击方法，比如病毒传播、弱口令、钓鱼邮件等，通过二维坐标（横坐标为资产，纵坐标为攻击向量）描绘出系统攻击面和风险形势，系统攻击面管理是系统有效性验证的物理基础和边界。同时通过系统自动化的攻击模拟验证从不同维度对资产风险量化和再评估，形成了可直接了解风险形势的安全视角。系统攻击面管理示意如图2所示。

a）搜集系统的资产信息IP、域名、主机、服务等，标记风险相关的数据分类，如暴露面类型、网络区域、资产归属方、南北向交互访问安全策略、开放端口。通过资产发现、智能爬虫、指纹识别发现关联资产并

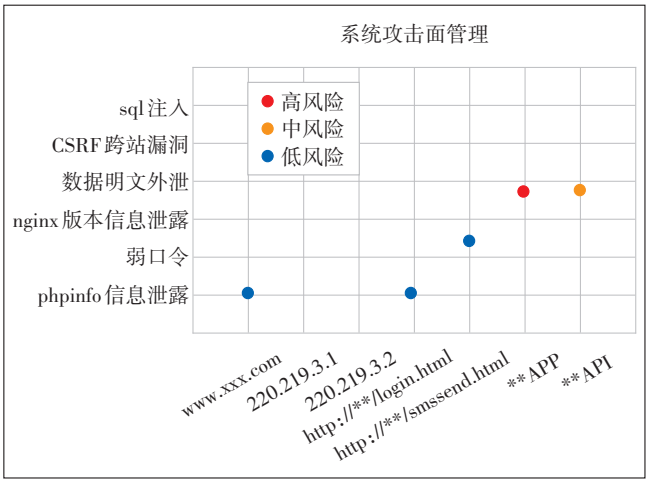

图2　系统攻击面管理示意

补充资产更细维度的信息，包括开放端口、操作系统、应用程序、插件、网络设备、应用供应链等信息。

b）基于识别的资产进行漏洞扫描、漏洞验证（多源扫描器交叉验证、poc验证），完成单漏洞的确认和初步风险值评估，绘制攻击面管理的二维坐标基础数据。

c）通过系统持续的攻击模拟模型，对漏洞联合利用和验证，进行漏洞多维度的风险评价，更新系统二维坐标中系统漏洞的风险评估等级及量化指标。

d）随着系统攻击面信息的挖掘，以及漏洞风险多维度持续叠加评估，系统的攻击面管理范围不断收敛，防止防御体系建设过度蔓延。

2.2 攻击场景知识库

通过每一次攻防演练，收录成功渗透目标的思路和专业黑客组织的攻击特征，并进行高度总结形成场景知识。攻击场景知识库为攻击模拟模型提供漏洞利用的样本数据和原型，同时为系统防御的有效性验证人员提供丰富的攻击案例和漏洞利用的方法思路。知识库积累过程如图3所示。

a）确立攻击场景的划分维度，可按攻击目标（终端、应用、APP、API、内网等）、漏洞利用的方式（弱口令、单漏洞、联合利用等）、漏洞利用的技术手段（口令爆破、php漏洞木马上传、传输数据篡改等）、攻击场景是否必须携带payload对业务有无影响等进行分类，合理的维度划分对知识库精准匹配和攻击模拟模型的迭代升级至关重要。

b）系统自动收集攻击成功案例生成知识库知识数据，从攻防对抗活动中自动搜集红队人员每一次的移动路径、方法、攻击成果信息进行数据存储，当红方

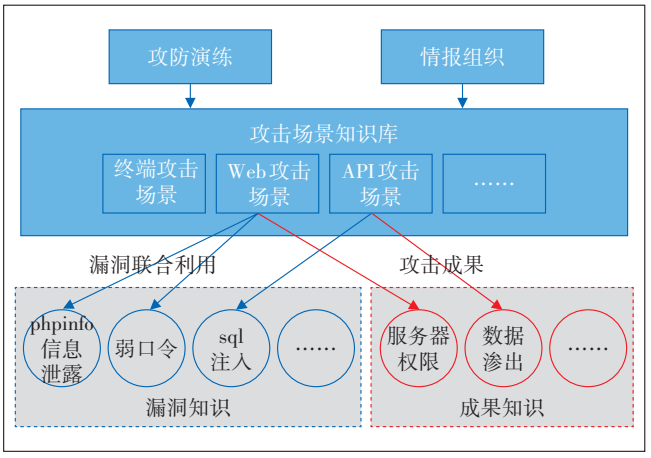

图3　知识库的积累过程

人员成功提权时系统自动反向匹配判断是否为新知识，新知识需要通过信息溯源生成方法、路径、关键结果等。

c）知识库通过对接情报组织，及时发现新的攻击案例和攻击行为。

2.3 攻击模拟模型

系统安全防御的有效性验证从以人工为主，逐渐转变为以机器为主，人工为辅的形式。通过对漏洞利用和验证方法的模型抽象，生成攻击模拟引擎，通过智能调度算法与关联分析模块对当前和历史产出的攻击结果分析，进行漏洞的迭代和联合验证，以达到具备一定专业水平渗透人员的思考方式。攻击模拟的调度及实现思路如图4所示。

a）攻击模拟引擎引入BAS技术，模拟自动攻击，类似于渗透人员使用各种渗透工具的过程，针对漏洞的理解、错误配置、用户特权，关联到一起形成攻击模拟引擎尝试的各种方案。通过对关键资产的攻击路径，确认关键的攻击点。

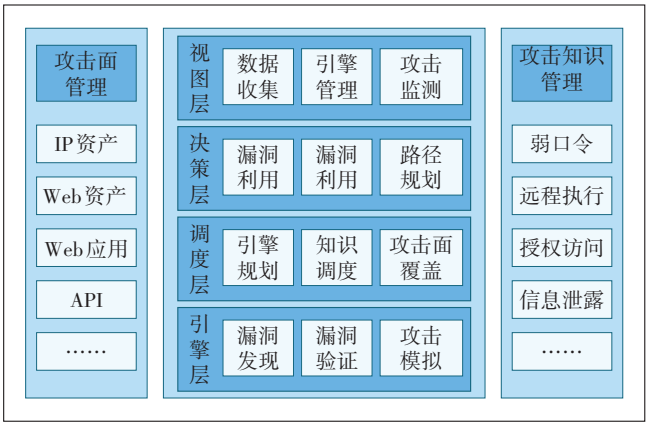

图4　攻击模拟的调度及实现架构

b）攻击模拟引擎的调度依赖于智能化的调度算法和对产出结果精确判断，在攻击过程中进行知识迭代，从而发现联合利用的知识项。采用PSO算法对验证结果进行信息共享，并通过攻击模拟引擎间的协作，对漏洞的深入理解和联合利用验证，以达到单点漏洞利用无法发现的业务风险点。

c）从攻击场景知识库中提取信息对称的攻击场景剧本，进行有监督训练。基于系统已知信息进行白盒攻击模拟验证，做到对系统暴露面的风险“心中有数”。

d）从攻击场景知识库中提取信息不对称的攻击场景剧本，进行无监督训练。对系统目标进行特定重点漏洞渗透，此时攻击模拟的过程全程黑盒，通过攻击模拟过程中的主动探测和分析，完成对目标的渗透。

2.4 攻击报告及复盘

攻击报告中包含攻击目标的全景信息，包括攻击的覆盖链路，发送的攻击报文以及回显信息等，针对攻击报告中产生的新的攻击面以及攻击知识进行标记，补充完善攻击面管理和场景知识库。

攻击报告不仅为使用者展示系统漏洞以及漏洞利用的全风险链路提供修复建议。更重要的是，以攻击者的视角验证系统的安全防御能力，以防御者的视角审视系统安全风险，实现未卜先知，防患于未然。

3 方案对比分析

3.1 系统风险管控

常规的有效性验证手段从静态验证到接近真实攻击的红蓝对抗活动，通过系统台账逐一检查确认，验证的过程高度依赖人员的渗透经验，随着活动持续时间的限制，验证的覆盖面也会随之缩减，系统风险的度量指标没有标准化，无法合理有效管控风险。

智能化的有效性验证通过系统主动探测、分析形成攻击面管理的资产数据范围，通过智能调度算法对目标进行攻击模拟验证，实现多维度、动态的风险的量化评估，对资产的漏洞进行分类分级管理，使系统风险度量准确和管理可控。

3.2 知识的传播

常规的验证手段通过渗透人员的知识储备、缜密的渗透思路、完备的渗透工具来完成对特定攻击目标验证，尤其对于新的攻击方法的大面积验证需要人力、物力、环境等，客观限制条件不利于攻击验证知识的传播。

智能化的有效性验证通过无监督的攻击模拟模型的学习探索，发现新的攻击知识，并通过有监督的攻击模拟模型的持续验证，新的攻击知识可以在环境中无约束地大面积应用，对系统攻击知识的信息进行快速核验。

3.3 验证的持续性

常规的验证手段需要向目标发送大量的模拟攻击报文，对目标可用性、系统配置以及系统数据有所影响，验证活动的时间、范围严重受限，验证活动无法持续。

智能化的有效性验证根据业务系统的可用性要求以及重要程度，控制攻击报文携带的payload，通过攻击模拟过程中对目标的配置和产生脏数据记录，验证动作结束时对上述配置和数据回滚，避免对业务系统产生影响，使验证的活动可持续。

4 总结

企业随着系统复杂度的提升，安全防御体系的管理难度也随之提升。对防御体系的有效性验证如果没有自动化的验证工具辅助或持续性的验证，系统的防御体系的有效性验证也将成为另一种负担。本文将BAS进行系统性的应用和组织，实现有效性验证的覆盖面可控、活动的可持续、攻击过程的可视化。

无论BAS还是其他的攻击模拟技术，技术的成熟度仍面临着巨大的挑战，如何适应日新月异的技术与业务环境，构建出完整的面向企业实际场景的防御的有效性验证，仍需要无数安全人的持续努力，但是智能化的有效性验证技术显然是未来发展趋势。

参考文献：

[1] PEROZZI B，AL-RFOU R，SKIENA S. DeepWalk：online learning of social representations[C]//Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York，USA：Association for Computing Machinery，2014：701-710.

作者简介：
杨丽丽，毕业于合肥工业大学，学士，主要从事网络安全技术方向的研究工作；刘果，毕业于武汉理工大学，学士，主要从事网络安全技术的研究工作；戚大强，毕业于中国药科大学，学士，主要从事网络安全技术的研究工作；张彬，毕业于昆明理工大学，硕士，主要从事大数据的研究工作；高贯银，毕业于北京师范大学，硕士，主要从事网络安全相关系统的研发及研究工作。