网络空间资产测绘与攻击面管理的技术分析

文◆北京禹宏信安科技有限公司 石 磊 雷 雪

引言

在我国当前数字化转型稳步推进的背景下，网络安全形势呈现出复杂化状态，为了进一步强化网络安全防御能力，应当积极探索网络空间资产测绘与攻击面管理的可行技术手段。本文以网络空间资产测绘功能为切入点，探讨了网络空间攻击面管理威胁态势，重点分析了网络空间资产测绘与攻击面管理技术要点，以期发挥新型网络安全技术的最大优势。

1 网络空间资产测绘功能

网络空间资产测绘技术指的是全方位系统化梳理、识别、定位网络空间资产的一种现代化手段，其借助多元化方法收集整合网络空间关于应用程序、系统、服务等方面的资产信息，进而打造出高度完整化的网络空间资产地图。其根本目的是扫描网络资产而构建自动化网络空间资产数据库，其功能涵盖以下 5 点。其一，资产发现。在大面积扫描与探测过程中识别出网络已知、未知、已备案、未备案、边缘化与隐藏化资产。其二，资产识别。细致化识别与分类所发现的资产，具体为服务应用、操作系统类型、开放端口等信息。其三，漏洞扫描。以资产识别结果为出发点，配合使用漏洞扫描技术，检测资产漏洞，找出其中隐藏的安全风险。其四，数据可视化。可通过地图、图表等形式可视化、直观化地呈现出扫描识别结果，使用户能够清晰理解与深层次分析网络空间资产整体状况与实际分布状况[1]。其五，资产管理。其具备资产管理功能，可为用户网络资产管理与维护提供可行化建议，具体涵盖资产漏洞跟踪修复、资产清单管理、安全策略规划等。

2 网络空间攻击面管理威胁态势

网络空间攻击面管理的威胁态势十分严峻，随着网络攻击技术的持续发展，攻击手段更新速度加快，安全漏洞出现频率更高，企业承受更为突出的攻击面风险，攻击者借由 APT 攻击、勒索软件、攻击链攻击以及 AI 技术等手段威胁企业的数据安全、业务安全以及品牌形象。一方面，从全球网络攻击威胁态势来看，首先，勒索软件攻击仍处于持续化高发状态，攻击目标持续扩大，涉及金融、政府、教育等核心领域。攻击者往往使用加密数据和破坏系统等方法勒索高额赎金，导致业务中断，使受害者遭受重大经济损失。其次，漏洞利用攻击仍然占据主导地位。攻击者可利用漏洞和弱点渗透并摧毁目标系统，这种攻击方法不需要大量投资，却具有出色效率，攻击者可以很容易地使用自动化工具和技术在短时间内快速攻击大规模目标。最后，攻击关键信息基础设施数量持续增多，APT 攻击更加活跃化。另一方面，从国内网络空间资产测绘与攻击威胁态势来看，首先，勒索软件攻击呈高速增长态势，攻击目标的针对性更强。攻击者已不再满足通过加密数据来勒索赎金，而是向

【作者简介】石磊（1980—），男，山东乐陵人，本科，研究方向：网络安全、攻防演练、应急溯源、数据安全。
【通讯作者】雷雪（1987—），女，河北廊坊人，本科，研究方向：网络安全。

国内关键信息基础设施攻击与大型企业高价值目标攻击倾斜，窃取机密数据后，以威胁被攻击者公开的方式而加大其赎金支付压力[2]。其次，攻击链攻击是攻击面管理的关键难点问题。攻击者围绕软件漏洞、人员疏忽与第三方服务攻击目标，此种攻击方式的隐蔽性和破坏性都很高，若攻击成功，整个供应链都会陷入巨大的安全威胁。再次，网络空间资产测绘技术和国际高水平技术仍有较大差距，资产暴露情况较为严峻，仍被黑客、APT 组织等重点关注，这些组织会针对网络空间中暴露出的脆弱资产发起攻击。最后，由于网络空间资产测绘的漏洞精准定位能力仍需加强，资产漏洞评估速度较慢，尚未实现全生命周期响应监控，由此埋下了较大安全隐患。

3 网络空间资产测绘与攻击面管理技术要点

3.1 可视化技术

网络空间资产测绘与攻击面管理技术的研发，需以网络空间资产测绘与攻击面的根本特征为出发点。攻击面是指系统中可被攻击者利用开展攻击的各类元素集合，包括操作系统、安全漏洞、网络配置等内容。基于这一特征，攻击面管理可充分借助多种技术手段，其中可视化技术的应用尤为关键。在开展攻击面管理工作时，通过可视化技术对网络攻击面进行直观展示，有助于强化企业安全队伍的风险感知能力，从而能够在较短时间内识别网络空间中的风险问题。可视化技术以图形、图表等直观化形式为呈现载体，能够清晰、全面地展示企业的网络架构、系统漏洞以及被攻击路径等核心信息，为攻击面管理提供必要的方向与思路支持。此外，在攻击面管理过程中，若将可视化技术与机器学习算法和大数据分析技术相结合，还可实现对网络安全状态的实时化、持续化监测，并同步具备报警与响应功能，从而最大限度地降低攻击面造成的后果与不良影响。

3.2 资产探测技术

为防止网络空间资产测绘与攻击面管理存在局限性，应着重推动资产探测技术的落地应用，同时运用多类别探测技术引擎，使其充分发挥互补作用，为全面采集网络空间资产信息创造必要条件。其一，远程扫描技术。该技术的核心功能是，在网络可达的状态下，可以在短时间内完成资产信息收集任务。其作用的发挥需遵循相关技术要求，支持分布式子网探测，可快速识别 150 余种协议，满足资产指纹特征管理的根本要求。但是，该技术存在一定局限性，即对指纹准确度的依赖较高，无法实现资产信息的全面采集。其二，轻量代理技术。该技术能够深层次、精准地采集资产的多元化信息，为资产安全事件处置奠定基础。其可适配主流操作系统，CPU 和内存占用率较低，且具备自主式调节与一键关停功能。

3.3 资产指纹技术

资产指纹技术主要围绕五大维度层面开展工作，能够有效提高资产识别精准化系数。首先，管理域。该维度主要承担资产管理属性描述功能，可支持对 16 大类、158 小类的资产进行描述，能让资产特征记录更为详细，实现资产扩展属性自定义。其次，业务域。该维度聚焦于资产的业务属性描述，通过对资产业务进行合理分域，可科学高效地划分资产的重要程度、责任归属与风险等级。最后，拓扑域、风险域、时间域也各有侧重。拓扑域主要围绕资产的邻近信息进行采集；风险域着重开展漏洞与异常风险的采集工作；时间域则侧重于对资产全生命周期的属性进行描述，通过识别资产归属、风险与异常情况的方式，在时间维度上实现对资产的全过程持续监控。

3.4 资产识别技术

在网络空间资产攻击面管理中，资产识别技术是一项关键技术，涉及多种技术类型，应用要点也十分丰富。

其一，主动扫描技术。该技术通过发送 ping、TCPSYN 等网络探测数据包，对目标网络的开放端口与活动主机进行探测处理，同时系统化识别主机的服务类型与操作系统等关键参数信息。在应用此技术时，可依托 Nmap 工具对目标网络进行扫描，在扫描过程中识别获取主机、操作系统、开放端口、服务版本等网络重点信息。其二，被动扫描技术。该技术与主动扫描技术有着显著区别，其通过监听 ARP 请求、DNS 查询等网络流量来识别网络内的活动主机和开放端口，同样可以精准识别主机的关键信息。企业在开展攻击面管理工作时，可选择使用 tcpdump 工具监听网络流量，并根据反馈的监听信息分析出网络流量的相关信息。其三，网络空间测绘技术。该技术是扫描与探测互联网上资产的重要手段，具体涉及网站、域名以及 IP 地址等，以此为根据识别企业的外部资产与攻击面。其四，威胁情报技术。在攻击面管理过程中，通

过多元化威胁情报收集与分析的方式，准确识别与企业资产密切相关的威胁信息。这里的威胁情报包括攻击事件、漏洞信息与恶意软件等。企业应加大对威胁情报平台的订阅力度，不仅能够高效获取最新出现的漏洞信息，还能及时识别出企业资产中容易受到消极影响的资产，从而及时采取相应的防御措施。其五，Agent 技术。该技术以 Agent 程序为实现载体，将程序安装在终端设备上以后，负责终端设备的信息采集任务，采集的核心信息包括硬件配置、软件安装以及操作系统等，同时将采集到的信息第一时间上传至攻击面管理平台，为统筹制定科学可行的攻击面管理方案提供有力支持。

3.5 攻击面识别技术

攻击面识别技术的功能作用在于对企业面临的各类安全风险与威胁进行准确化识别与深层次分析，涵盖配置缺陷、数据泄露、弱口令以及漏洞等方面。其一，配置检查。采取科学化的配置检查工具检查网络空间资产状况，从中找出资产在配置方面的缺陷与不足，具体包括网络设备所含有的弱口令以及账户默认等安全风险。其二，数据泄露检测。在数据泄露检测工具的有力支撑下，持续监控企业网络流量，重点判定在文件上传、下载、邮件发送等环节是否出现数据泄露行为。其三，漏洞扫描。使用漏洞扫描工具完成企业网络空间资产扫描工作，从而找出资产中隐含的安全漏洞。例如，通过漏洞扫描器扫描服务器漏洞，在发现服务器漏洞的同时对其风险等级加以评估。其四，敏感信息识别。开展网络空间资产扫描工作时，应配合使用敏感信息识别工具，该工具是攻击面识别技术中的重要单元模块，通过它可发现资产中的机密文件、数据库密码、源代码等敏感信息的存储位置与访问权限。其五，威胁情报应用。在威胁情报平台获取攻击事件、恶意软件以及漏洞信息等最新的威胁情报，将其作为开展攻击面管理的根本依据。通过威胁情报平台订阅漏洞信息，便于第一时间掌握最新的漏洞信息，同时识别出企业资产中受到漏洞影响与干扰的相关资产。

3.6 攻击面入侵与模拟技术

攻击面入侵与模拟技术（BAS）的要点可细化为模拟攻击、攻击路径分析、安全验证、安全评估四大方面。其一，模拟攻击。该技术可对不同类型的攻击进行模拟，具体包括模拟攻击者借助社会工程学等手段获取初始访问权限、模拟攻击者进入内网后的横向移动状态、模拟 APT 攻击和勒索软件攻击等，以此作为企业安全防御体系有效性评估的根本依据。其二，攻击路径分析。全面分析攻击者会使用的攻击路径，同时识别出攻击路径中的薄弱环节。借助 BAS 手段，可分析掌握攻击者从互联网向企业内网关键服务器发起攻击的路径，并精确识别定位出攻击路径上的薄弱点，如弱口令以及未做补丁处理的漏洞等。其三，安全验证。该技术可满足对安全控制措施有效性的验证需要，重点围绕攻击入侵检测系统以及防火墙等措施展开。通过 BAS 模拟出攻击者对防火墙的攻击情况，测试判断出防火墙对攻击流量的实际拦截能力。其四，安全评估。该技术可深层次评估企业的整体安全状况，并给出可行的改进建议[3]。以模拟攻击结果为基本导向，系统化评估判定企业安全防御体系是否处于稳定的安全状态、是否具备优越的安全防御能力等，同时向企业提出相关安全措施，如在原有基础上进一步加大企业职员安全意识培训力度、优化改进当前的安全策略以及积极引入与合理部署安全设备等。

结语

网络空间资产测绘与攻击面管理关乎企业 IT 基础设施对于资产风险和安全风险的实际抵御能力，主要围绕可视化技术、资产探测技术、资产指纹技术、资产识别技术、攻击面识别技术、攻击面入侵与模拟技术展开，由此构建出具备敏锐力、感知力、阻断力的安全主动防御体系，做到高效化、准确化识别各类风险问题。

引用

[1] 曾颖明.基于攻击面的网络隐蔽信道安全检测技术研究[D].西安:西安电子科技大学,2024.

[2] 弭希超.面向软件定义网络饱和攻击的流表管理技术[D].北京:北京邮电大学,2023.

[3] 王雪莉,蔡均平,陈刚.网络空间攻击和防护策略运用研究[J].网络安全技术与应用,2020(10):9-10.