

多步攻击检测技术综述

王笑语^{1,2}, 龚晓锐^{1,2}, 章 秀^{1,2}, 程子俊^{1,2}

¹中国科学院信息工程研究所 北京 中国 100093

²中国科学院大学网络空间安全学院 北京 中国 100049

摘要 随着网络空间的不断发展和防御能力的不断增强,网络攻击行为变得越来越多样化和复杂化。在这种演变中,多步攻击已经成为网络攻击的主要方式之一。多步攻击是具有相同最终目标的多个原子攻击以特定逻辑序列组成的有目的的攻击。相较于单步攻击,多步攻击的时间跨度更长、隐蔽性更高、危害性更大。因此,多步攻击的检测是网络安全领域关注的重点课题。近年来,研究人员提出了大量针对多步攻击的检测技术。本文对这些研究进行了全面的梳理和总结,首先给出多步攻击的定义和特点,并列举多步攻击检测面临的挑战以及检测技术的发展阶段;随后本文从不同角度对检测技术进行了分类,根据使用的数据来源将多步攻击检测技术分为基于报警信息、基于日志关联和基于混合信息三种类型,每种数据源内,根据检测流程分为预处理、整合、关联、攻击检测四个步骤。本文从多个角度对这些检测技术进行了详细分析,系统地总结了每种类型的研究在数据集使用、实时性效果、处理步骤、是否生成关联图以及评估方法等方面的细节。最后,本文列举了可用于实验的数据集,并探讨了未来研究可能的方向。本文期望通过分析现有的多步攻击检测技术,为后续多步攻击检测研究提供有益参考。

关键词 多步攻击; 攻击检测; 报警关联; 溯源图

中图法分类号 TP393.08 DOI号 10.19363/J.cnki.cn10-1380/tn.2026.05.14

A Survey of Multi-step Attack Detection

WANG Xiaoyu^{1,2}, GONG Xiaorui^{1,2}, ZHANG Xiu^{1,2}, CHENG Zijun^{1,2}

¹ Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

² School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract With the continuous evolution of cyberspace and the strengthening of defensive capabilities, attack behaviors are progressively becoming more diverse and complicating. Based on these trends, multi-step attacks have emerged as a dominant modality for orchestrating cyberattacks. A multi-step attack refers to a purpose-driven action comprising multiple atomic attacks that are sequenced in a specific logical order and aimed at achieving the same ultimate goal. Compared with single-step attacks, multi-step attacks have a longer time span, heightened levels of concealment, and greater potential for damage. Consequently, the detection of multi-step attacks has become a key focus in the field of network security. In recent years, researchers have proposed a large number of detection techniques tailored to address multi-step attacks. This paper conducts a comprehensive review and synthesis of these research. The paper initiates by providing the definition and characterization of multi-step attacks. It then highlights the challenges encountered in detecting multi-step attacks and presents the developmental stages of detection techniques. Subsequently, this paper classifies the detection technology from two perspectives. Based on the data sources employed, multi-step attack detection techniques are categorized into three primary types: those grounded in alert information, those relying on log correlations, and those harnessing hybrid information. Within each data source category, techniques are further classified according to the detection process, which includes preprocessing, integration, correlation, and attack detection. This paper performs a detailed analysis of detection techniques from diverse aspects, and systematically summarizing the particulars details of each research, including elements such as the dataset employed, real-time effectiveness, position in the processing pipeline, generation of correlation graphs, and evaluation methods. Finally, this paper lists the datasets available for multi-step attack detection experimental evaluation, and explores potential directions for future research. Through analyzing the existing multi-step attack detection technologies, this paper expects to provide valuable references for the future research on multi-step attack detection.

Key words multi-step attack; attack detection; alert correlation; provenance graph

通讯作者: 龚晓锐, 硕士, 正高级工程师, Email: gongxiaorui@iie.ac.cn。

本课题得到国家自然科学基金(No. 61802394, No. 61902396), 中国科学院战略性先导科技专项项目(No. XDC02040100)和青促会人才项目的支持, 也得到中国科学院网络测评技术重点实验室和网络安全防护技术北京市重点实验室的支持。

收稿日期: 2021-04-07; 修改日期: 2021-06-28; 定稿日期: 2023-08-22

1 引言

随着网络空间的不断发展,攻击行为也逐渐多样化。通常所说的“攻击”(attack)指的是单步攻击,也称为原子攻击,即不可拆分的原子恶意行为,如SQL注入^[1]、跨站脚本执行(Cross Site Scripting, XSS)^[2]等,这些攻击只需一步操作即可达成攻击目的。然而,随着网络结构的复杂化和防御方防御能力的增强,攻击目标(如数据库服务器、核心服务器等)通常位于内部网络,而且受到多种安全产品的保护。这种情况下,攻击者仅通过单一简单步骤往往无法达成攻击目的,而是需要组合多个攻击步骤来实现攻击目的,这种攻击称为多步攻击(Multi-step attack),也称作多阶段攻击(Multi-stage attack 或 Multistage attack)。

多步攻击是攻击者为实现特定攻击目的发起的有计划的攻击,是将各个攻击步骤以一定的逻辑顺序组合的攻击序列。比如, Mirai 僵尸网络病毒^[3]首先使用已感染“肉鸡”进行物联网设备的扫描,随后对潜在的存活主机进行爆破登录,成功登录后上传恶意代码,并根据命令发动分布式拒绝服务(distributed denial of service, DDoS)攻击。整个攻击过程包含扫描、暴力破解、上传恶意软件、恶意软件执行等步骤。Mirai 僵尸网络的影响巨大,在2016年11月感染的设备达到了600,000台,攻击者利用这些感染的设备对域名解析服务商发动拒绝服务攻击,造成2016年10月21日美国大面积断网^[4]。典型的多步攻击是高级持续性威胁(Advanced Persistent Threat, APT),指有专业知识和丰富资源的攻击者,通过多种不同的途径在攻击目标的信息基础设施建立初始据点,一步步入侵进而达成其攻击目标^[5]。APT攻击具有强烈的政治背景或经济目标,造成的危害十分严重,如2015年底乌克兰配电公司遭到攻击导致全国大范围断电,波及约225000用户^[6];从2013年起,Carbanak组织对银行进行攻击,窃取了超过十亿美元的资金^[7]。

多步攻击的特征是攻击过程包括了至少两个原子攻击,这些原子攻击之间存在逻辑关系。在攻防双方的对抗模式下,多步攻击是攻击者与防御能力逐渐增强的防御者进行博弈而采取的必然行动。因此,防御方想要在攻防博弈中占据优势地位,就必须具备有效的多步攻击检测能力。

多步攻击检测目前已经成为网络安全领域关注的重点问题。相比于传统的单步攻击,多步攻击更加复杂,时间跨度更长,隐蔽性更高。攻击步骤之间可

能会相隔较长时间,在此期间,攻击者潜伏在目标网络中等待用户触发特定事件或收集用户信息。多步攻击检测与单步攻击检测的区别体现在每个步骤之间的关联上。如何通过网络流量信息、终端日志信息以及各个安全防护设备产生的攻击报警等信息对攻击者行为进行还原是多步攻击检测的重点。目前已有的研究综述大部分是基于单步攻击,例如机器学习方法在入侵检测领域的应用^[8-11],基于网络的入侵检测技术及数据集^[12]等。这些技术应用于入侵检测系统(Intrusion Detection System, IDS),仅检测出单步攻击的异常或报警,每个攻击步骤之间的逻辑关系还需要进一步研究。

本文基于多步攻击的特点和检测挑战,对现有的多步攻击的检测方式进行研究。本文首先总结了多步攻击概念和特点,梳理分析多步攻击检测技术的发展过程。然后,对多步攻击检测方式进行多角度分类,将多步攻击检测根据数据来源分为基于报警信息、基于日志信息和基于混合信息三类,根据检测流程分为线索预处理、线索整合、线索关联、攻击检测四个步骤,对每一种方式进行深入分析与比较。最后,列举用于研究的数据集,并指出该领域未来可能的研究方向。

本文的组织结构如下:第2节对本文研究所用的背景知识进行阐述,并介绍多步攻击及检测方式的特点和发展阶段;第3~第5节分别介绍基于报警、基于日志、基于混合信息的多步攻击检测技术;第6节对多步攻击的检测技术进行讨论,包括各种检测方法优缺点对比、实验所用数据集、目前面临的挑战等,并展望未来可能的发展方向;第7节总结全文。

2 研究背景

本节首先介绍基础知识,接着列举典型的多步攻击案例,随后分析多步攻击的特点,并指出多步攻击检测面临的挑战。

2.1 基础概念

报警 多步攻击检测中的报警(alert 或 alarm)是指各种防护硬件或软件识别的恶意活动产生的信息。如网络入侵检测系统(Network Intrusion Detection System, NIDS)对网络通信中出现的攻击特征产生报警。报警中可能会出现误报和漏报,真实性需要多步攻击检测系统进一步分析。

日志 系统或应用程序记录系统操作或程序行为的文件。如Linux安全模块Audit^[13]和Windows安全模块^[14](Event Tracing for Windows, ETW)产生

的系统日志, Apache 服务器产生的访问日志等。与报警相比, 日志所需存储空间大, 但是包含的基础信息量更多。

事件 报警与日志的总称, 表示主机或网络中发生并被记录下来的动作。各种来源的报警和日志之间的格式不同, 因此事件通常是异构的。

攻击模型 攻击模型可以用于指导攻击步骤关联。常见的攻击模型包括杀伤链模型^[15]和 ATT&CK 模型^[16]。杀伤链模型由洛克希德-马丁(Lockheed Martin)公司^[17]提出, 将攻击过程分为 7 个步骤, 包括侦查跟踪、武器构建、载荷投递、漏洞利用、安装植入、命令与控制、目标达成。杀伤链模型仅定义了攻击各个环节的宏观框架, 对具体的攻击内容与行为没有统一的标准, 因此在杀伤链的基础上, MITRE 公司提出了对手战术及技术的通用知识库(Adversarial Tactics, Techniques, and Common Knowledges, ATT&CK), 介绍更加底层的攻击技术框架。ATT&CK 表现为一个矩阵, 横轴表示战术(Tactics), 是攻击者执行行动的理由, 按照典型攻击流程划分为多个攻击阶段, 如文件或命令执行, 持久化, 防御规避等。纵轴表示技术(Techniques), 代表攻击者通过执行动作来实现战术目标的方式, 如通过修改注册表的方式达到持久化的目标^[18]。与杀伤链模型相比, 除了增加了详细技术细节之外, ATT&CK 并没有线性顺序约束, 表示攻击者可以跳过或重复执行战术来达成目标。

2.2 多步攻击举例

多步攻击中的攻击行为有明显的阶段性和步骤性, 本节给出两个多步攻击案例, 一个是海莲花组织的 APT 攻击, 另一个是普通的多步攻击。

案例一: 境外黑客组织“海莲花”^[19](OceanLotus, 也称 APT-C-00, APT32)以感染并窃取目标计算机中的机密数据为目的。报告^[20]指出, 该组织首先对目标(某 Windows 主机)发送包含 ActiveMime 类型恶意文档附件的钓鱼邮件, 诱导目标用户打开附件并启用宏, 随后该附件创建两个计划任务, 第一个计划任务下载并执行 Meterpreter, 随后加载 Cobalt Strike BEACON 后门。第二个计划任务启动 APT32 的定制后门。后门与命令与控制端(Command and Control, C&C)进行通信, 执行横向移动、敏感信息回传等后续操作。这些攻击步骤环环相扣, 每个步骤完成不同的目标, 最后达到攻击目的。图 1 描述了海莲花组织攻击的流程。

案例二: 文献[21]给出了一次多步攻击行为案例的分阶段描述^[22]。第一阶段初始植入: 外部攻击者使

用 IRC 的远程代码执行漏洞, 使 Linux Web 服务器回连到攻击机的 4444 端口, 并上传恶意软件 trojan.exe 到/var/www 目录下。第二阶段恶意软件感染: Windows 客户机用户从 Web 服务器下载恶意软件 trojan.exe 并运行, 回连到攻击机, 使攻击者可以访问内网。第三阶段权限提升: 通过 trojan.exe 启动 notepad.exe 进程, 再次回连到攻击者, 获取管理员权限, 转储内存空间并枚举缓存的域控制器管理员凭据。第四阶段获取凭据: 利用从上一步中获得的域管理员的凭据, 连接到域控制器 Windows DC, 并通过 powershell.exe 回连到攻击机, 上传密码枚举工具 pwdump7.exe 或 wce.exe, 转储存储在域控制器内存中的所有用户信息。第五阶段数据泄露: 利用用户凭据, 连接到数据库服务器并下载数据库, 创建反向连接, 将数据传回攻击机。

作为典型的多步攻击, APT 通过侦查跟踪、武器构建、载荷投递、漏洞利用、安装植入、命令与控制、目标达成等一系列步骤, 最终达到窃取信息、破坏服务、控制系统等目的。应注意的是, 并不是所有的多步攻击都是 APT, APT 具有强烈的政治背景和组织性, 但多步攻击不限于此。政治背景和有组织的攻击等并不是多步攻击定义的必要条件。

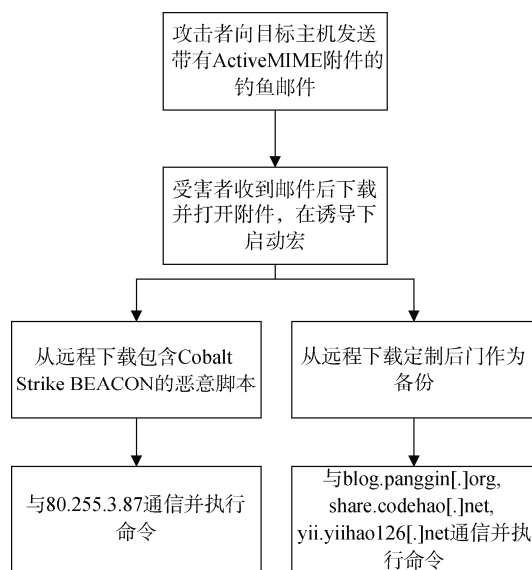


图 1 海莲花组织攻击流程举例

Figure 1 OceanLotus group attack process

2.3 多步攻击特点

多步攻击具有时间跨度大、隐蔽性高、目的性强等特点。

时间跨度大 攻击过程中, 攻击者的恶意软件会潜伏在目标网络中等待用户触发, 也可能在这段时间内收集信息。除攻击过程的时间长之外, 从攻击

开始到被攻击发现的过程也较长。报告指出,企业从被入侵成功到发现入侵的平均时间为 188 天,而最长可达 1655 天^[23]。在此期间,攻击者可以在网络中潜伏以窃取机密信息。

隐蔽性高 攻击者可能会利用正常提供的服务完成攻击步骤,如通过枚举的方式获取系统中安装的软件和软件版本的列表^[24]。这种方式并不会产生报警信息,增强了攻击者的隐蔽性。此外,在系统内部潜伏直到出现目标活动也提高了多步攻击的隐蔽性。

目的性强 多步攻击的目标较为明确,如对于工业控制领域,其目标在于攻击工业控制系统导致系统崩溃或停止运行^[25-26],而对商业机构则需要窃取秘密信息。较强的目的性表明多个攻击步骤之间存在逻辑关系,而非简单的时序组合。攻击者的每个步骤都是为了达到最终的信息窃取或破坏等任务而存在,因此可以通过分析逻辑关系发现攻击的不同阶段。

多步攻击与传统的单步攻击有很大不同,检测方式也有较大区别。单步攻击的检测侧重异常的发现,属于发现攻击“点”;而多步攻击的检测侧重于评估攻击步骤之间逻辑性,目标是发现攻击“线”和“面”。表 1 总结了多步攻击和单步攻击的特点及其在检测上的区别。

表 1 多步攻击与单步攻击特点及检测区别
Table 1 Characteristics and detection differences between multi-step attacks and single-step attacks

攻击类型	攻击特点	检测重点
单步攻击	一次完成,易被检测,目标简单	特征检测,异常检测
多步攻击	时间跨度大,隐蔽性高,目的性强	各步骤之间的逻辑关系,发现完整的攻击过程

2.4 多步攻击检测挑战

多步攻击检测面临的挑战包括时间跨度大造成日志和报警数据量增长问题和完整的多步攻击流程的还原问题。

时间跨度大造成日志和报警数据量增长 在多步攻击执行的较长时间跨度中会产生大量的报警信息和日志记录。为保证网络的安全性,网络中部署了大量的边界防火墙设备、入侵检测系统、防病毒软件等安全防护设备或软件。经调查,在 750 名网络安全和 IT 专业人员中,有 78% 依靠 50 种以上的离散产品来解决安全问题,37% 的人使用 100 多种安全工具^[27]。这些安全产品大多数采用传统的特征匹配或统计分析方法检测已知攻击,会产生大量的误报。报告指出,大部分组织平均每月会产生超过 10000 条报警信息,

超过 52% 的报警都是误报,超过半数的组织需要人工分析所有报警^[28]。文献[29]指出审计日志在服务器和客户端中分别以 3.18GB/天和 1.2GB/天的速度增长。快速增长的日志造成存储和分析的难度,如何从海量数据中发现多步攻击的线索成为检测的挑战。

完整的多步攻击流程的还原 多步攻击检测的目标是尽可能发现完整的攻击过程,但数据中的漏报和误报增大了检测的难度。多步攻击手段的隐蔽性造成安全设备对一些攻击步骤的漏报。当前大多数检测设备采用特征匹配进行攻击检测,这种检测落后于攻击手段的变化,也会导致漏报的产生。同时,为减少漏报,厂商往往降低安全产品的阈值,这又导致很多正常的网络活动被识别为异常事件,会产生大量误报。多步攻击的难点在于如何发现并聚合属于同一次攻击流程的线索,并通过上下文信息发现线索之间的逻辑关系,还原完整的攻击流程。

2.5 多步攻击检测发展阶段

与单步攻击不同,多步攻击的检测需要发现各步骤的逻辑关系,因此仅检测一个攻击步骤的研究不在本文的讨论范围之内,如对横向移动的检测、对异常流量的检测等。结合文献[30],多步攻击检测领域的研究关键词包括报警关联(Alert Correlation)、攻击场景重建(Attack Scenario Reconstruction)、攻击故事重建(Attack Story Reconstruction)、APT 检测(APT Detection)、取证分析(Forensic Analysis)等。这些关键词的核心特点都是发现攻击步骤之间的详细关系,以检测或预测多步攻击。我们研究文献的范围包括知名期刊或会议里多步攻击检测领域相关的代表性文章,因为多步攻击检测领域的时间跨度较大,本文选取 20 年内的多步攻击检测相关研究文章。

多步攻击检测发展历程中出现的代表性研究如图 2 所示。基于多步攻击检测领域代表性文章,从 2001 年至 2023 年,多步攻击检测的发展可以分为三个阶段:以报警关联为主阶段、多步攻击检测探索阶段、以日志及多源信息为主发展阶段。2001~2005 年属于以报警关联为主阶段,这一阶段里研究者通过分析报警的相互关系发现多步攻击,大量的报警关联代表性文章发表于这一阶段,如基于因果关系、基于结构的报警关联等,报警关联技术的研究路线和框架在该阶段构建完成;2005~2017 年是多步攻击检测的探索阶段,这一阶段中,报警关联技术进一步发展,同时研究者也在探索多步攻击检测的新方式,例如首次提出结合报警与日志进行攻击过程的检测;2017 年至今是以日志及多源信息为主的多步攻击检测阶段,因为存储能力和计算能力的提高,在这一

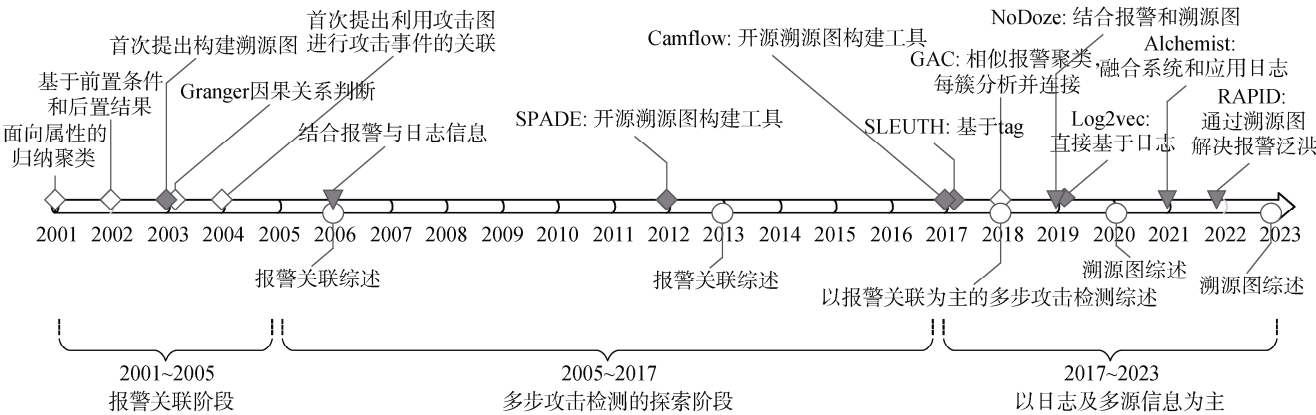


图 2 多步攻击检测代表性研究及发展阶段

Figure 2 Representative research and development stages of multi-step attack detection

阶段研究者使用具有更多信息含量的系统日志进行检测, 同时结合了报警、应用日志等多源数据进行信息的优化和扩充。

从检测阶段可以看出, 多步攻击检测的数据源包括目标网络的网络流量信息、终端日志信息以及各个安全防护设备(如防火墙、网络入侵检测系统、主机级入侵检测系统等)产生的攻击报警。根据使用的数据来源, 多步攻击检测可以分为基于报警信息、基于日志关联和基于混合信息三种方式。基于检测的流程, 多步攻击检测分为线索预处理、线索整合、线索关联、攻击检测四个阶段。每项研究在各个阶段有不同的侧重, 但是总体来说, 线索关联阶段在多步攻击检测过程中是至关重要的阶段。本文从多步攻击检测所用的数据源出发, 对检测流程进行分析。

2.6 相关工作

多步攻击检测相关的综述性文章的研究范围分为报警关联和溯源图关联两类, 当前已有的综述文章仅从一个层面或角度分析多步攻击检测研究, 尚未有完整概括多步攻击发展历程及技术的文章。表 2 概述了本文与其他综述性文章在研究目标、研究范围等内容上的区别。文献[31-32]的研究目标是

报警关联, 文献[30]的研究目标虽是多步攻击检测, 但其聚焦于报警关联, 本质属于报警关联综述的范畴。文献[33]和文献[34]的研究目标是溯源图的应用。本文研究多步攻击检测技术, 从多步攻击的角度对相关文献进行梳理。

3 基于报警的多步攻击检测

报警是网络内各个安全监控软件产生的报警事件, 包括系统的可疑行为和错误操作。随着防御水平的提高, 系统内的安全监控软件也更加多样化, 如基于网络的入侵检测系统 NIDS、基于主机的入侵检测系统(Host Intrusion Detection System, HIDS)、应用级防火墙等。这些安全监控软件会产生大量代表单步攻击的报警, 如何处理分析这些报警成为基于报警的多步攻击检测的主要研究点。报警分析的一般流程是报警预处理、报警聚合、报警关联。多数研究聚焦在报警聚合和报警关联两个阶段。

3.1 报警预处理

报警预处理阶段统一定义报警的格式。不同检测引擎产生的报警有不同的表达方式, 但是存在相同字段, 如源 IP 地址、目的 IP 地址等。基于报警的

表 2 本文与相关综述文献对比

Table 2 Comparison with related survey

文章	[31]	[32]	[30]	[33]	[34]	本文
时间	2006	2013	2018	2021	2023	2023
研究目标	报警关联	报警关联	多步攻击检测	溯源图	溯源图	多步攻击检测
研究范围	报警关联	报警关联	报警关联	溯源图	溯源图	多步攻击检测
发展阶段概述	无	无	无	有	无	有
数据源	无	无	无	无	无	有
检测流程分解	有	有	无	有	有	有
评价指标	无	无	无	无	无	有

检测第一步是将由不同检测引擎产生的报警调整为同一格式。目前报警的标准格式是入侵检测消息交换格式^[35](Intrusion Detection Message Exchange Format, IDMEF), 用于在入侵检测和入侵防御的软件之间以 XML 格式进行信息交互^[36-40]。IDMEF 格式的报警信息包括创建时间、检测时间、源节点信息、目标节点信息、报警名称等。IDEA^[41](Intrusion Detection Extensible Alert)基于并扩展了 IDMEF, 新增了报警类别字段, 创建报警类别列表, 通过已有的类别名称来描述安全事件, IDEA 使用 json 格式。除标准格式外, 很多研究使用自定义的报警格式, 如将报警整理成包含源 IP 地址、目标 IP 地址、源端口、目标端口等一系列属性的结构化数据。

3.2 报警缩减

庞大的报警数量是对多步攻击检测的一项挑战, 通过缩减报警数量可以减少后续关联分析的工作量。报警缩减的对象包括两种: 相似报警和低风险报警。相似报警通过相似度报警聚类的方式进行聚合。文献[42-45]将在时间间隔内具有相同报警类型的报警合并, 生成报警集合。文献[46-47]把报警根据 IP 和端口进行连接, 形成带权重的图, 使用派系过滤方法(Clique Percolation Method, CPM)算法进行聚类, 得到的每一簇为一次单步攻击。文献[48-50]定义了报警包含的属性类型是分类属性、数值数型、时间属性和字符串属性, 并提出使用算法, 对报警进行聚类分析, 以识别使报警持续出现的根本原因。基于相似度的报警聚合只能聚合相似报警, 无法对误报进行过滤。

对于低风险告警, 可以通过排序的方式过滤, 留下高价值报警。文献[51-52]分别通过有监督的加权支持向量机分类算法(Weighted Support Vector Machine, WSVM)和无监督的孤立森林异常检测算法(Isolation Forest, IF)进行报警排序。DeepCASE^[53]和 Context2Vector^[54]认为报警的排序与其上下文相关, 分别通过 Encoder-Decoder 架构和 LDA2VEC 算法提取上下文特征, 将报警表示为向量, 实现报警的分类、聚类目标。对误报的过滤还可以由关联算法辅助进行, 如在关联中未与其他报警有联系的报警为误报、没有匹配到攻击图中的漏洞的报警为误报等。

3.3 报警关联

在多步攻击检测中报警关联的目标是发现报警之间的逻辑关系, 一些面向报警关联的综述文献^[12,32]将基于相似度的报警聚合归为报警关联, 在多步攻

击检测领域, 基于相似度的方法仅能缩减报警数量, 无法发现报警之间的因果关系, 不属于多步攻击的发现攻击步骤的部分, 故本文没有将其划为报警关联。因此, 报警关联的方法包括基于因果关系的报警关联和基于结构的报警关联。

3.3.1 基于因果关系

基于因果关系的报警关联挖掘报警之间的逻辑关系, 包括基于先验知识的关联和基于统计信息的关联两种方式。

基于先验知识的方法根据预先定义的规则将报警进行连接, 文献[55-57]提出了超级报警(hyper-alert)的概念, 超级报警是一个三元组, 包括事实(fact)、前置条件(prerequisite)、后置结果(consequence)。事实是指出现在前置条件和后置结果中的变量集合, 如 IP 地址。前置条件是指一组基于事实的逻辑公式, 代表只有满足该公式的攻击才会成功。后置结果也是一组基于事实的逻辑公式, 表示攻击成功后攻击者获得的能力或环境状态的改变情况。符合前置条件的报警信息可以扩展出后置结果, 组合成超级报警。各个超级报警之间通过前置条件和后置结果的匹配进行连接, 最后可以得到超级告警的关联图。如图 3 所示, 矩形表示前置条件和后置结果, 花括号表示一个超级告警。

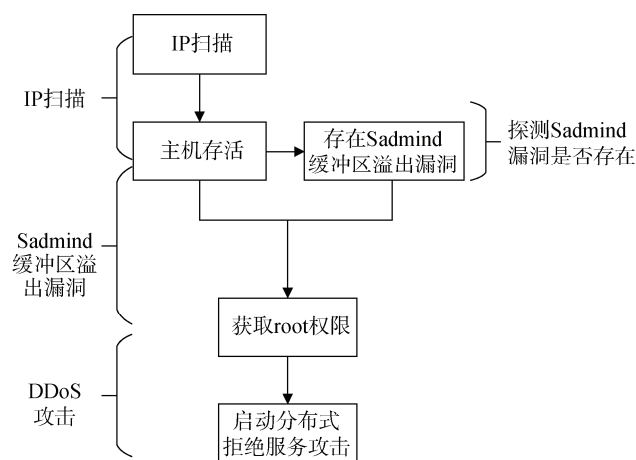


图 3 超级告警实例^[49]

Figure 3 Hyper-alert sample^[49]

基于先验知识的报警关联具有较好的可解释性, 并且只需要提前编写每一种攻击的前提条件和可能造成的结果, 无需描述完整的攻击流程。这种方法可以挖掘不同的攻击组合, 但是只能够发现已知攻击, 且需要安全专家手动或半自动编写规则, 关联的效果与规则的质量密切相关。同时, 多步攻击过程时间跨度大, 产生的报警数量多, 关联图在搜索条件或

结果时资源消耗大, 且会产生路径爆炸的问题。

基于统计信息的多步攻击检测是通过对已有报警进行分析, 使用机器学习技术, 学习其线索分布情况, 建立概率分布模型, 挖掘攻击的频繁模式和时间序列, 用于检测攻击或预测下一步攻击。文献[42]认为将所有攻击都表示为精确的先验知识不够灵活, 因此提出通过结合先验知识判断安全状态, 从而在贝叶斯网络上进行关联关系的推理, 并分配概率。文献[43]引入时间序列模型, 对报警进行 Granger 因果关系判断是否关联。文献[44]认为通过方法[42-43]关联之后的报警可能会因为有些攻击未检测到而形成孤立的关联图, 因此提出了一种基于攻击树和贝叶斯网络进一步关联报警并识别攻击意图的方法。文献[58]提出一种基于因果知识网络(Causal Knowledge Net, CKN)的攻击路径预测方法。通过告警映射到已经发生的攻击行为序列, 动态推断攻击者能力等级, 调整概率分布, 最后实时预测攻击路径。胡倩^[59]提出通过贝叶斯网络进行多步攻击的预测, 首先通过对攻击序列训练集采用数据发掘的方式得到因果关系关联规则和贝叶斯网络参数的概率分布, 然后基于关联规则构建因果贝叶斯攻击场景图, 最后基于场景图进行参数概率推理和概率预测计算, 从而进行攻击预测。文献[60]从报警事件中挖掘频繁子集, 发现攻击模式。首先根据报警的源和目的 IP 生成图结构, 再使用 Bit-AssocRule 算法^[61]定期挖掘频繁模式, 但是挖掘频繁子集的方法不能发现不频繁的攻击。

文献[62]选取报警的 6 个特征, 基于两种不同的神经网络方法, 即多层感知器(Multi-Layer Perceptron, MLP)和支持向量机(Support Vector Machine, SVM)进行报警关联, 并将报警存入警报关联矩阵(Alert Correlation Matrix, ACM), 最后基于该矩阵生成攻击报警图。文献[45]对聚合之后的报警使用事件片段挖掘算法发现可能的报警序列, 随后通过攻击决策树学习生成关联权重矩阵。GAC^[47]对聚合后的单步攻击报警簇打标签, 将其分为一对一、一对多、多对一、多对多四种类型, 代表四种不同类别的攻击。并随后将簇之间的源 IP 和目的 IP 进行统计分析, 得到每簇之间的关联。Jiang 等人^[63]将报警数据映射为攻击意图, 作为隐式马尔可夫模型(Hidden Markov Model, HMM)中隐藏的状态信息, 并采取群体智能优化算法 LVPSO 对 HMM 优化, 实现多步攻击检测、意图识别和攻击预测。文献[64]设计 seq2seq 模型, 使用长短期记忆网络(Long Short-Term Memory network, LSTM)从长报警序列中学习长期依赖性, 并部

署了编码器-解码器架构, 以充分利用从输入报警序列中学到的可用知识。

3.3.2 基于结构

基于结构的多步攻击检测方式认为多步攻击对象与目标网络结构和网络中资产的价值有关, 因此通过抽象网络结构规划或预测攻击者的动作。攻击图^[65]是对漏洞、资产、网络拓扑进行表示, 将可能的攻击路径以图的形式进行呈现。文献[66]首次提出利用攻击图进行攻击事件的关联^[29], 指出攻击图入侵事件提供了上下文支撑, 将报警关联分为离线和在线两个过程。如图 4 所示, 离线过程中生成攻击图, 在线过程将攻击事件映射到攻击图的节点中, 形成事件路径, 实时还原攻击事件之间的因果关系。首先人工分析漏洞利用并将其建模, 结合网络拓扑模型, 进行攻击路径分析, 生成攻击图以及攻击之间的距离。在线过程中, 将报警与漏洞利用对应, 计算报警之间的距离, 并生成攻击路径。

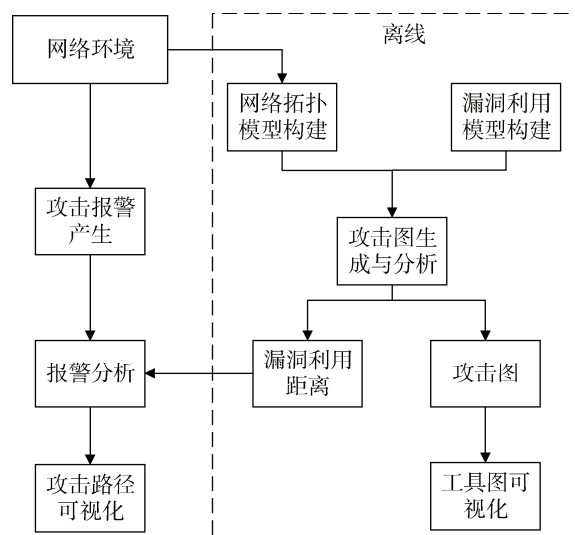


图 4 文献[63]的工作模式

Figure 4 Work model architecture in Ref.[63]

文献[48]使用从攻击图构建的队列图(queue graph)进行报警的关联和下一步攻击动作的预测。文献[67]对多步攻击进行建模, 扩展了攻击树结构, 增加有序并列关系, 为节点增加生存时间属性和攻击级别属性, 提出增强的并行自动机, 并引入攻击概率属性描述执行操作或子目标的难度。当出现新报警时, 将预期报警与检测到的报警进行比较, 以确定是否产生报警。文献[68]基于报警在攻击图上的图形距离和时间距离进行报警的关联。文献[69]使用着色 Petri 网表示多步攻击, 并进行资产评估和攻击场景预测。

表 3 基于报警的多步攻击检测
Table 3 Multi-step attack detection based on alert

类别	方法	文献	时间	数据集	实时性	处理步骤			关联图	评估
						报警预处理	报警缩减	报警关联		
报警 缩减	聚类	[49]	2001	自建	否	属性定义与 层次分类	基于属性归纳聚 类近似算法	无	无	案例介绍
		[50]	2003	自建	是	属性定义与 层次分类	层次聚类	无	无	案例介绍
	排序	[51-52]	2019,2021	自建	否	无	WSVM, IF	无	无	定量分析压缩率
		[53]	2022	自建	否	无	Encoder-Decoder	无	无	定量分析压缩率
		[54]	2022	自建	否	无	LDA2VEC	无	无	定量分析压缩率
报警 关联	先验 知识	[55-57]	2002-2005	DARPA 2000	否	无	有	基于先验知识	有	关联效果定量评估; 关联图展示
		[42]	2004	GCP	否	IDMEF	聚类	贝叶斯网络	有	关联效果定量评估; 结果图展示
		[43]	2005	GCP DARPA 2000 DEFCON CTF 9	否	IDMEF	聚类	Granger 因果关系	有	关联效果定量评估; 关联图展示
		[44]	2005	GCP	否	IDMEF	聚类	贝叶斯网络和 攻击树	有	关联效果定量评估; 结果图展示
	基于 统计	[58]	2016	自建	是	无	无	因果知识网络	有	预测结果图展示
		[59]	2019	DARPA 2000	是	无	无	贝叶斯网络	有	预测结果图展示
		[60]	2012	DARPA 2000	是	IDMEF	聚类	挖掘频繁子集	有	关联图展示
	报警 关联	[62]	2006	DARPA 2000	是	无	无	神经网络	有	关联矩阵展示; 关联图展示
		[45]	2012	DARPA 2000+自建	是	无	合并报警集合	报警片段生成, 决策树	无	权重矩阵展示; 报警片段展示
		[47]	2018	自建	否	无	CPM 算法	基于数学统计	无	聚类评估; 场景识别
		[63]	2019	DARPA 2000	否	无	无	LVPSO-HMM	无	参数展示; 效果评估
	基于 结构	[64]	2021	DARPA 2000+入侵 检测数据集	否	独热编码	无	seq2seq 模型	无	关联效果定量评估
		[66]	2004	自建	是	无	无	报警映射攻击 图	有	攻击图展示; 事件距离分析
		[48]	2006	DARPA 2000	是	无	无	报警构建攻击 队列	有	预测结果图展示; CPU 占用; 内存占用; 耗时
		[67]	2007	自建	否	无	无	扩展攻击树	无	噪声影响下的结果
		[68]	2008	自建	是	无	无	报警距离计算	有	关联结果展示; 算法性能展示
		[69]	2012	DARPA 2000	否	无	无	着色 Petri 网	有	预测结果展示

3.4 评价指标

因为使用方法的不同, 报警分析评价指标也不同。报警分析的评估方式包括对算法步骤分解的测试和在真实场景下的整体测试。评估时针对具体的步骤进行定量分析或定性分析。对报警缩减的评估集中在定量分析报警聚合的比例、与已知压缩算法的比较等。报警关联时定量分析关联的准确度、关联算法复杂度与耗时等, 定性展示关联图检测出的多步攻击过程。文献[55]提出了报警关联结果的完整性和可靠性计算公式, 并在两个 DARPA 数据集上进行了测试, 与 RealSecure 工具生成的报警结果进行对比。文献[47]从包含单个攻击的数据集和包含多种

攻击的数据集两个层次对报警过滤和报警聚类算法进行了评估。

3.5 小结

基于报警的多步攻击检测对报警信息进行处理与关联, 发现报警之间的逻辑关系。表 3 介绍了文献中使用的数据集、实时性、阶段技术及评估方式。但是基于报警的检测面临报警的漏报和误报问题, 报警关联效率与安全防护设备的攻击检测能力密切相关。攻击者使用零日攻击或与正常操作无异的攻击方式时, 不会产生报警信息, 则缺少了攻击步骤, 对检测系统的关联能力提出了挑战。同样, 当正常行为也会触发报警时, 能否识别误报成为基于报警的

多步攻击检测的难点。

4 基于日志的多步攻击检测

基于日志的多步攻击检测是近年来受到关注的检测方式。日志指的是操作系统和应用软件产生的操作记录,如进程读取和写入文件等。与报警相比,日志包含的信息量更大,但是日志记录没有是否是攻击的标记,需要进行深入分析。基于日志的多步攻击检测分为直接基于日志检测和基于溯源图的检测两部分。

4.1 直接基于日志

直接基于日志的方法是指直接对日志信息进行分析,无中间表示。根据处理过程,直接基于日志的方法分为日志预处理、日志压缩、日志关联和攻击检测四个阶段。

4.1.1 日志预处理

日志是半结构化数据,在进行后续处理前需要将其转换为结构化数据。经典的日志处理方法是提取其消息通用表示,消除日志中的可变部分,提取的格式一般为键值对: (“消息模板”, “参数值”)。提取使用分析源代码、分析日志、直接使用正则三种方式。文献[70]认为表示消息模板的常量通常占据日志序列的大部分,而参数值仅占小部分,因此提出了基于最长公共子序列的日志解析器,以流的方式将非结构化日志消息解析为结构化消息模板和参数值。文献[71]通过分析程序源代码里的日志打印语句中的模式来提取消息模板。文献[72]通过正则表达式进行日志的提取。除提取日志模板之外,另一种日志的预处理方式是将日志规范化表示为 N 元组的模式,以便后续处理^[73-74]。

4.1.2 日志压缩

因为日志中的消息模板存在重复,占用大量存储空间,目前主流的文件压缩方法不适用于半结构化的日志格式。文献[75]提出 Logzip, 将每条日志消息分为日志头和日志内容两个部分,从日志内容中自动提取日志消息固定模板,随后将模板和参数分别进行映射,最后使用通用压缩算法进行压缩。由 Logzip 生成的半结构中间表示可以直接用于各种下游日志挖掘任务。

4.1.3 日志关联

直接基于日志的关联大部分使用了多个日志文件,关联时对日志的相同属性进行关联,因此在本文中将其划分为基于混合信息的多步攻击检测范畴。如文献[74]对 6 种日志进行建模,并提出了 29 个关联特征,从不同的维度对日志进行关联。因为包

含了多种日志类型,直接基于日志关联的研究在 5.3 节系统日志与应用软件日志结合和 5.4 节异构事件整合中介绍。

4.1.4 攻击检测

文献[76]提出 Deeplog, 使用深度学习对日志进行异常检测。Deeplog 通过方法^[70]进行日志预处理,使用 LSTM 算法对日志消息模板序列的执行路径异常进行判断,之后对日志参数值进行预测与异常判断。这种方法的使用前提是用户的活动是有规律的,并且需要大量的标注数据。Log2vec^[73]根据定义的 10 条启发式规则将日志生成异构图,通过随机游走提取每个节点的上下文,把由节点的上下文构成的路径看作自然语言处理中的句子,随后进行嵌入表示,通过聚类发现攻击。

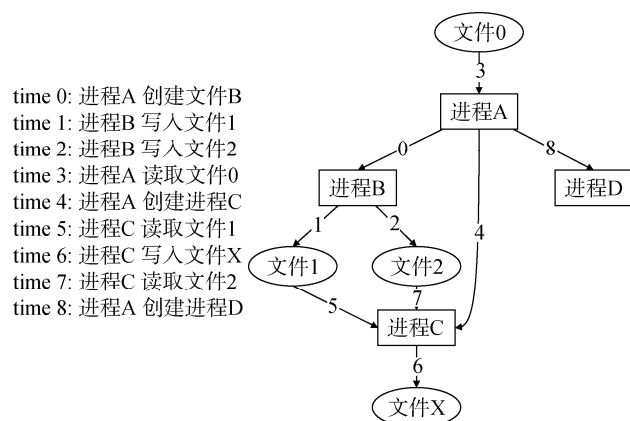
直接基于日志方式在进行攻击检测时通常是基于人工智能算法发现异常。这种异常检测可以发现日志中存在的异常行为,但无法详细描述出现异常的详细原因及攻击路径。

4.2 基于溯源图的检测

基于溯源图的检测是在预处理阶段将日志生成溯源图,之后做基于溯源图的分析。基于溯源图的检测包括日志预处理(溯源图生成)、日志缩减(溯源图优化)和攻击检测三个阶段。与报警关联相比,因为日志在预处理生成溯源图时被关联,所以去除日志关联这一步骤。

4.2.1 溯源图生成

目前大部分只依靠日志进行多步攻击检测的研究都使用日志溯源图表示日志。日志溯源图(provenance graph, 也称作 dependence graph)是一个有向图,挖掘进程、文件与文件名之间的因果依赖关系,为攻击溯源提供了丰富的上下文信息。文献[77]在 2003 年首次提出构建溯源图,定义了进程与进程之间、进程与文件之间、进程与文件名之间的基于系统调用的依赖关系。进程之间的依赖是进程创建、共享内存、通信等进程之间直接的影响关系。进程与文件的因果关系指进程与文件之间存在的操作关系,如文件读写执行等。进程与文件名之间的关系是指以文件名为参数的系统调用,如文件的打开、创建、重命名等。如图 5 所示,左边是日志中的系统调用事件序列,右边是基于日志生成的溯源图。在溯源图中,文件用椭圆表示,进程用矩形表示,网络 socket 用菱形表示。溯源图除用于多步攻击检测外,还可以用于恶意软件的运行时检测^[78-80]等研究,与本方向无关,故不做赘述。

图5 溯源图模型^[77]Figure 5 Provenance graph model^[77]

溯源图中会出现环路, 如一个程序连续读写同一个文件, 或两个进程进行双向交互。环路的存在会影响算法对图结构的处理, 因此文献[81]对溯源图增加了版本(version)的概念, 检测是否存在环路, 当存在环路时为相应对象创建新版本。基于版本产生的溯源图是有向无环图。

文献[82-83]开源了两个用于实时生成溯源图的工具 SPADE 和 Camflow, 其中 SPADE 对 Audit 和 Windows ETW 产生的审计日志进行处理, Camflow 是一个 Linux 内核模块, 捕获数据并将系统的执行表示为有向无环图。

研究人员通常通过对溯源图从检查点(detection point)进行前向(forward tracking)和后向(back tracking)遍历, 构建攻击路径。检查点是指被认定为恶意的文件或进程, 通常是攻击行为暴露的位置。

4.2.2 溯源图优化

多步攻击所用时间周期较长, 日志的增长速度快, 生成的溯源图较大, 直接基于溯源图进行攻击检测会出现依赖爆炸的问题。因此许多工作围绕如何提高对溯源图分析效率展开, 包括溯源图细化、日志冗余压缩、日志语义抽象压缩三种方式。

1) 溯源图细化

溯源图细化的目标是解决依赖爆炸问题。依赖爆炸问题是指, 在长时间运行的进程中, 从操作系统的角度来看, 随着日志的不断增长, 每个输出事件都依赖于所有先前的输入事件。溯源图细化包括两种方式: 程序切分和因果推理。

通过程序切分缩减依赖的原理是长时间运行的进程在其生命周期内可能与其他实体具有依赖, 但其中仅有少数与攻击有关。例如, 一个 Firefox 进程在其生命周期内可能会访问许多页面, 而只有一个

页面与恶意软件下载有关。文献[84]认为, 长期运行的程序通常会处理很多个相互独立的输入, 因此提出 BEEP 系统, 将二进制程序切分为处理特定对象的事件循环单元(unit), 每个 unit 处理不同的输入, 这样可以有效地避免路径爆炸带来的效率问题。文献[85]认为 BEEP 所用的事件循环单元的语义级别低, 会出现大量冗余, 因此提出了原型系统 MPI, 对源码进行注解并配合静态分析来直接切分出逻辑子任务。文献[86]改进了 BEEP 的做法, 使用轻量级的内核模块 Tracepoints^[87], 对 unit 的事件进行污点分析, 减少日志占用空间和分析运行时长。

文献[88]认为程序切分的缺点在于需要复杂的二进制分析, 因此基于因果关系缩减依赖提出了 MCI, 通过 LDX 程序因果关系推理引擎^[89]分析程序构建系统调用依赖模型, 利用该模型分析日志中的事件关系。

2) 日志冗余压缩

针对日志的量级问题, 日志冗余的压缩是多步攻击检测所需的重要步骤。日志压缩的目的是在不影响分析精度的条件下, 尽量减少日志中因果关系的数量。文献[29]提出 LogGC, 对系统日志文件进行分析, 将事件分为输入(input)事件、输出(output)事件和终结(dead-end)事件三种类型。终结事件只影响一个对象, 并且不再创建新的依赖, 如删除文件, 终止进程。LogGC 认为大多数(80%以上)的被删除的文件都是临时文件, 在其生命周期过程中只与一个进程有关, 这类文件的删除对进程分析没有帮助, 可以进行回收。在实验中, LogGC 平均可以压缩处理 92% 以上的日志。文献[90]认为两个对象节点之间的多个同类型的边可能是重复的, 如进程多次读取文件, 并提出了保留依赖的数据缩减算法(Causality Preserved Reduction, CPR), 通过前向和后向搜索减少重复事件。文献[91]通过观察进程启动情况, 认为当一个进程启动时, 通常需要加载库文件和资源文件进行初始化, 这些文件中不包含有用的依赖信息, 也就是说, 合并这些只读文件节点不影响依赖分析的准确性。因此提出基于模板的日志缩减技术, 根据文件访问模式使用 FP-Growth 算法生成模板, 构建有限状态机合并文件事件。文献[92]认为上述压缩方法减少的是分析人员认为不太可能使用并因此可以删除的事件, 输出的日志是近似日志。并提出对近似日志的评价标准: 无损压缩、保留因果关系、保留攻击关系。最后提出一种基于正则的近似日志压缩方法 LogApprox, 在消除冗余的同时保证因果关系和攻击场景的保存。

3) 日志语义抽象

文献[93]提出 WATSON, 通过嵌入模型 TransE 对系统日志进行抽象化的表示, 从日志事件的上下文提取出行为的语义, 识别并聚合相似行为, 减少重复分析。WATSON 使用知识图的方式表示异构事件。通过抽象化表示, 可以从低级审计日志中识别出高层次系统行为, 减少日志分析人员的工作量。

4.2.3 攻击检测

如何对溯源图进行处理用来检测攻击是多步攻击检测的目标, 当前共有四类方法进行溯源图上的攻击检测。

1) 基于统计

文献[94]通过分析系统调用生成对象实例图, 基于实例图构造贝叶斯网络, 并根据适当的感染传播模型为每个节点生成条件概率表(Conditional Probability Table, CPT), 通过深度优先搜索算法(Depth First Search, DFS), 在实例图中保留具有高概率的节点以及其所互联的边, 突出显示零日攻击路径。文献[95]提出 PRIOTRACKER, 基于系统在未出现攻击行为之前的正常活动, 对系统事件的优先级进行排序, 根据正常事件与异常事件之间的区别来优先研究异常操作。优先级与事件的常见程度、事件的投入产出、事件中数据的重要程度(是否被读过、是否被写过)有关。偏离参考模型的行为就是攻击行为。该方法的局限性在于需要保证参考模型构建时系统未被攻击。

文献[96]也基于统计分析异常事件发现攻击, 该方法的数据源包括报警与日志, 因此将在下一节进行介绍。

2) 基于语义

文献[97]提出 HOLMES, 构建中间层高级场景图(High-level Scenario Graph, HSG)将溯源图与 ATT&CK 模型中 APT 的攻击阶段关联, 解决底层日志数据与高层次攻击链语义理解之间的鸿沟。为弥补语义理解上的差距, HOLMES 在日志和攻击阶段之间构建了基于 ATT&CK TTP 的中间层, 并通过规则进行日志的抽象化。攻击检测时, 分析各阶段的严重性, 计算整体攻击的重要性。文献[98-99]结合报警与日志, 基于 ATT&CK 报警语义构建高层次图, 将在下一节进行介绍。

3) 基于异常检测

UNICORN^[100]使用溯源图嵌入进行异常检测, 首先建立一个已知良性的溯源图模型, 将图表示成为直方图并生成固定大小的图概要(graph sketches)。系统运行时, 将从系统启动到目前为止所产生的溯

源图模型与良性模型进行定期聚类比较, 如果偏离了该模型, 那么就认为发生了攻击。基于异常的检测方式可以发现攻击, 但是无法分析该攻击的具体步骤, 且异常检测易出现误报。

4) 基于标签

文献[101]结合攻击者的动机与方法, 提出基于标签(tag)的溯源图, 定义可信度标签和机密性标签, 并设置标签传播策略和报警触发策略, 最后从报警的触发点对溯源图进行前向和后向的遍历。文献[102]改进了标签的定义和传播方式, 提出数据标签和主体标签, 并且丰富了数据和代码上的标签传播策略。标签的引入细化溯源图的数据流和控制流, 减少了路径爆炸的问题。

4.3 评价指标

基于日志的多步攻击检测技术对算法或系统的评价指标包括性能评估、效果评估、结果图展示等。

通过性能评估证明本研究的运行效率。运行效率指该算法运行时占用的时间、内存占用、CPU 占用等。效果评估指发现攻击的效果, 如经过处理的溯源图表达攻击的准确性, 是否包含关键节点等。与报警关联相同, 直观地通过图的方式展现发现的攻击过程也是评估时常用的方式。

评价时通常在同一场景下横向比较多个算法, 如文献[95]将文献[77]作为基准线在准确率上进行比较、文献[102]与其之前的工作^[101]在同一场景下的报警触发数进行了比较。除进行定量效果的评估之外, 大多数研究还进行了案例的探讨, 通过详细描述攻击过程, 结合经过处理后得到的溯源图直观表示研究的效果。

4.4 小结

表 4 总结了基于日志检测的代表性工作。基于溯源图的多步攻击检测可以发现主机内攻击的详细过程, 为发现多步攻击提供了新方向。但是溯源图的生成和处理过程中占用的运行资源较多, 如何高效处理溯源图是该领域研究的重点。此外, 完整的攻击过程通常跨越多个主机, 因此需要关联网络数据与主机数据才能发现整个攻击的过程。因此跨数据源的关联是未来的发展方向。

5 基于混合信息的多步攻击检测

基于混合信息多步攻击检测是指整合多种信息进行多步攻击的检测, 这里的信息是指可以用于检测的有效知识, 除报警信息、日志信息之外, 还包括威胁情报信息等。基于混合信息的关联方式多样, 因此这里以数据源做区分, 具体的检测阶段在表格中呈现。

表 4 基于日志信息的多步攻击检测
Table 4 Multi-step attack detection based on log

类别	方法	文献	时间	数据集	实时性	处理步骤			攻击场景呈现	评估
						日志预处理 (溯源图生成)	日志压缩 (溯源图优化)	攻击检测		
直接基于日志	直接基于日志	[76]	2017	日志集	否	有	无	基于异常图嵌入+	无	性能评估; 效果评估
		[73]	2019	日志集	否	建模为 5 元组	无	聚类算法	无	性能评估; 效果评估
	日志缩减	[84]	2013	自建	否	有	程序切分	无	有	优化效果展示; 性能评估; 效果评估
		[85]	2016	自建	否	有	程序切分+污点分析	无	有	优化效果展示; 性能评估; 效果评估; 与 BEEP ^[84] 对比评估
		[86]	2017	自建	否	有	程序切分	无	有	优化效果展示; 性能评估; 效果评估; 与 BEEP ^[84] 、LogGC ^[29] 对比评估
		[88]	2018	自建+ DARPA TC	否	有	因果推理	无	有	优化效果展示; 性能评估; 效果评估; 与 BEEP ^[84] 对比评估
		[29]	2013	自建	否	基于 BEEP ^[84]	移除临时文件	无	无	优化效果展示; 性能评估; 效果评估
		[90]	2016	自建	否	有	CPR	无	无	性能评估; 效果评估
		[91]	2018	自建	否	有	FP-Growth 算法	无	无	性能评估; 效果评估
		[92]	2020	DARPA TC	否	有	基于正则	无	无	优化效果展示; 性能评估; 效果评估
基于溯源图	日志语义抽象	[93]	2021	自建+ DARPA TC	否	知识图	启发式移除可能会引起路径爆炸的部分	无	无	识别效果展示; 性能评估; 效果评估
		[94]	2016	自建	否	有	无	基于统计发现异常	有	高级场景图展示; 效果评估; 阈值选取; 性能评估
		[95]	2018	自建	否	有	无	基于统计发现异常	有	结果图展示; 各场景下的性能与效果
	攻击检测	[97]	2019	DARPA TC	是	有	无	基于语义	有	结果图展示; 效果评估; 性能评估
		[100]	2020	DARPA TC	是	有	无	基于异常	无	效果评估; 性能评估
		[101]	2017	DARPA TC	是	有	通过减少内存占用提高效率	基于标签	有	结果图展示; 各场景下的性能与效果
		[102]	2020	DARPA TC	是	有	无	基于标签	有	以 SLEUTH ^[101] 为标准的对比; 结果图展示; 性能展示

5.1 报警信息与系统日志信息整合

文献[103]对文献[77]提出的 BackTracker 进行跨主机拓展, 提出跨主机的报警和日志关联, 使用溯源图为报警提供补充信息, 从报警处开始对溯源图进行后向和前向的遍历。文献[104]认为报警关联效果依赖于报警的质量, 当报警出现误报时可能会产生错误的关联, 因此应整合报警信息和溯源图, 使用系统级依赖发现报警之间的关系。首先分析报警信息识别与报警对应的操作系统对象, 根据操作系统对象之间的依赖关系确定报警是否相关, 同时可以发现漏报的攻击。文献[96]提出 Nodoze, 为每个报警生成溯源图, 根据事件发生的频繁程度计算路径事件异常评分, 对报警信息进行排序, 区分真实报警与虚假报警, 并生成报警依赖图呈现多步攻击。

RAPID^[105]通过结合报警与日志数据, 构建实时报警分类系统。该方法引入 waypoint 作为先前任务中已经探索过的溯源图中的重要节点, 其属性和严重性评估结果作为攻击知识在任务之间共享。对新警报进行分类时, RAPID 根据已知 waypoint 为该报警分配优先级, 并使用新学习的上下文和经过的时间更新优先级分数, 实现警报分类任务的资源动态分配。SteinerLog^[106]基于情报规则和基于异常生成报警, 将报警映射到溯源图中, 并把从含有报警的溯源图中提取攻击相关子图的过程抽象为 prize-collecting Steiner-tree(PCST)问题, 目标是找到包含的告警最多, 并且所有告警之间的距离之和不超过阈值的子图。SteinerLog 还能够结合网络流量数据, 检测跨主机的横向移动。文献[107]提出了一个开源平台 zeek-

osquery^[108], 将 zeek^[109]入侵检测系统的报警输出与 osquery 主机监视器^[110]结合, 实时收集、处理和关联网络和主机数据。使用 socket 以五元组的形式抽象表示一个网络数据流, 包括双方 IP 地址、端口以及网络协议。与 socket 相关的文件描述符和进程 pid 作为 socket 的 ID。在关联过程中, 通过 IP 地址识别数据流的发送与接收方, 在双方的主机上根据 pid 识别对应的进程信息。

威胁模型如 ATT&CK 矩阵等带有攻击阶段等语义信息, 因此能够补充更多的高层次语义信息。文献[98]认为目前基于溯源图的分析对攻击行为的刻画过于底层, 无法呈现攻击者的攻击行为战术信息, 因此提出 RapSheet, 使用端点检测软件(Endpoint Detection and Response, EDR)收集日志信息并根据 ATT&CK 规则产生报警, 将溯源图和报警映射到战术溯源图中(Tactical Provenance Graph, TPG), 该图的节点表示报警事件。TPG 抽象表示溯源图中的攻击事件, 向分析人员展现高级别的攻击战术情况。最后, 通过通用攻击模式枚举及分类(Common Attack Pattern Enumeration and Classification, CAPEC)中的定义与分级进行威胁分数的计算。文献[99]针对当前各类方法所用数据结构不统一的问题, 提出 KRYSTAL 框架, 基于本体整合各类数据源, 生成统一的 RDF 溯源图。在生成的图中可以模块化地集成多种最新技术, 如基于 SPARQL 查询的标签传播、前向后向遍历等。同时, 将 ATT&CK 矩阵等背景信息引入 RDF 溯源图, 从低级事件图抽象到更高级别的技术和战术, 可以使攻击调查更加高效。

5.2 威胁情报信息与系统日志整合

文献[111]提出 POIROT, 首先将安全专家整合的结构化或半结构化的 OpenIOC^[112], STIX^[113], MISP^[114]信息, 生成一张查询图(query graph), 然后利用子图匹配的方法从溯源图中寻找匹配的相关子图, 从而发现威胁。POIROT 允许安全专家通过威胁指标(Indicator of Compromise, IOC)生成查询图去判断自己的公司是否受到攻击, 但是 POIROT 只能检测经过提前处理的威胁情报信息, 无法检测未知威胁。此外, 该方法需要安全专家根据攻击行为手动生成查询图。为实现该过程的自动化, Extractor^[115]和 AttacKG^[116]基于 APT 报告生成查询图, 实现非结构化攻击报告到结构化溯源图的自动化处理。

5.3 系统日志与应用软件日志整合

文献[74]认为之前的工作只关注一种日志, 所以缺乏对整个攻击的全局把控, 多阶段攻击模式留下的任何痕迹在时间和空间上分散在不同受害者机器

上的许多单独日志中, 并且日志收集过程依赖于重量级的日志系统, 这会带来不小的性能开销。因此提出了 HERCULE, 基于社交网络的启发, 将入侵分析模型化为社区发现问题, 提出了一种多维度权重图, 识别了 15 个知名的 APT 家族。

文献[117]提出基于系统日志的溯源图缺少了部分高级语义信息, 如电子邮件地址、HTTP 应答码等。为了解决这一问题, 提出了全局溯源图(universal provenance), 融合应用程序日志和系统日志。通过分析应用程序二进制文件, 生成控制流图, 提取日志相关字符串, 将应用程序日志整合进溯源图中。

文献[118]提出 Alchemist, 融合应用程序日志和审核日志。ALchemist 将日志整合成包含 20 个字段的统一格式, 结合推理引擎 Datalog, 预定义日志融合规则推导新关系, 最后生成减少了依赖的溯源图。这种方式通过从系统与应用日志中推导出 unit 信息, 不需要额外的二进制分析。

5.4 异构事件整合

文献[119]对报警事件、应用日志事件、系统日志事件等异构事件进行形式化定义, 并且对其之间的依赖关系进行定义与分析。通过形式化的定义, 可以挖掘事件之间的逻辑关系。通过对该图从报警节点开始进行前向和后向的遍历寻找该报警的因果关系图。文献[120]使用高交互蜜罐网络作为大规模捕获和收集多步攻击的工具, 收集原始流量有效载荷、可执行文件和蜜罐日志, 通过规则将其建模为通用事件, 通过属性关联事件, 结合检测规则生成攻击图。将攻击图作为输入进行聚类 and 分类, 判断多步攻击的属性。该方法可以发现新的多步攻击。

EDL(Event Description Language)是一种攻击特征检测语言, 最早由 Meier^[121]提出, 后来由 Jaeger^[122]进行了改进^[123]。EDL 使用着色 Petri 网构造节点序列来直观表示不同事件的串联。文献[124]提出基于污点图(taint graph)的污点传播自动提取多步攻击检测 EDL 的方法。除 EDL 外, 能够进行多步攻击描述的语言还有 STATL^[125](State Transition Analysis Technique Language)、CAML^[126](Correlated Attack Modeling Language)等。除对攻击事件进行描述外, EQL^[127](Event Query Language)、AIQL^[128](Attack Investigation Query Language)、SAQL^[129](Stream-based Anomaly Query Language)提供了对攻击事件的查询语言。

5.5 小结

表 5 总结了基于混合信息的多步攻击检测技术。基于混合信息的多步攻击检测将各种信息进行融合,

表 5 基于混合信息的多步攻击检测

Table 5 Multi-step attack detection based on mixed data sources

数据源	文献	时间	数据集	实时性	处理步骤				评估
					线索预处理	线索缩减	线索关联	攻击检测	
报警信息与系统日志信息整合	[103]	2005	自建	否	无	无	字段连接	前向搜索	结果图展示; 效果评估; 性能评估
	[104]	2006	自建	否	报警前因后果生成关联图; 溯源图生成	映射日志, 过滤误报, 补充漏报	基于时间戳的映射	判断线索依赖关系的真实性	结果图展示; 效果评估; 性能评估
	[96]	2019	自建	否	无	通过分析过滤误报	直接映射	基于统计	结果图展示; 效果评估; 性能评估
	[105]	2022	DARPA TC	是	溯源图生成	分析溯源图缩减无关报警	溯源图关联报警	可中断的基于优先级的调查	结果图展示; 效果评估; 性能评估
	[106]	2022	DARPA OpTC	否	溯源图生成	分析溯源图缩减无关报警	溯源图关联报警	PCST	结果图展示; 性能评估
	[107]	2020	自建	是	报警和日志建模为 5 元组	无	属性相同即连接	无	性能评估; 效果评估
	[98]	2020	自建	是	无	[90]和自定义规则	ATT&CK	CAPEC 分数	结果图展示; 效果评估; 性能评估
	[99]	2022	DARPA TC	否	自建本体模型	溯源图缩减	ATT&CK	RDF 查询的标签传播	结果图展示; 效果评估; 性能评估
	[111]	2019	DARPA TC	否	威胁情报生成查询图	无	图匹配	无	查询图展示; 效果评估; 阈值选取; 性能评估
	[74]	2016	自建	否	属性字段预处理建模	无	字段连接	社区检测	社区发现结果展示; 效果评估
系统日志, 应用日志	[117]	2020	自建	否	程序控制流分析	无	全局依赖图	无	结果图展示; 效果评估; 性能评估
多维度日志	[118]	2021	自建+ DARPA TC	否	定义模型规范日志表示	无	推理引擎 Datalog	无	结果图展示; 效果评估; 性能评估与[96], [117]对比
异构事件	[119]	2019	自建	是	形式化定义	无	因果关系	无	结果图展示
蜜罐事件	[120]	2020	自建-蜜罐事件	否	高交互蜜罐捕获攻击信息	无	字段连接	聚类分类	结果图展示

发现攻击步骤之间的关联。这种检测方式符合人类对攻击的基础认知, 即每步攻击因操作不同, 会留下不同的痕迹, 这些痕迹可能会分属于不同的数据源, 因此需要将这些数据源整合起来进行多步攻击的发现。但是现有研究仅对某些数据进行整合, 如报警和日志记录的整合、日志记录和威胁情报的整合等, 缺乏一种将所有数据源整合的方式。

6 讨论

6.1 多步攻击检测方式对比

多步攻击的检测方式各有千秋, 表 6 对多步攻击检测各阶段所用技术做了总结分析。表 7 对各种多步攻击检测方法的优缺点做了简要阐述。由表可知, 目前尚未出现对多步攻击检测的完美的解决方式。

6.2 数据集

与普通的入侵检测相比, 多步攻击检测需要用到存在多个攻击步骤的攻击数据集, 因此许多用于入侵检测的数据集^[130-133]不再适用。研究中使用的多步攻击检测的数据集主要包括 DARPA 2000 LLDOS

表 6 多步攻击检测各阶段所用技术

Table 6 Techniques used in each stage of multi-step attack detection

阶段	技术
线索预处理	报警格式化; 溯源图生成; 线索模型构建
线索整合	报警聚合; 报警过滤; 日志压缩; 溯源图优化
线索关联	报警关联; 报警映射溯源图; 属性特征关联
攻击检测	报警关联图分析; 溯源图遍历
评估	视具体技术而定, 关联图表示最直观

表 7 多步攻击检测现有方法总结

Table 7 Summary of methods used in multi-step attack detection

类别	方法	优点	缺点
基于报警信息	基于先验知识	基于预先定义的规则, 生成超级报警, 将前置条件和后置结果关联	可检测多步攻击, 反映攻击本质语义关系
	基于统计信息	基于对目标观测一段时间之后的统计知识	无须先验知识, 直接挖掘线索之间的关系, 可以发现未知攻击模式
	基于结构	首先对目标网络生成攻击图, 再根据攻击图的特性关联线索	准确率高
基于日志信息	直接基于日志	日志预处理后, 机器学习检测异常	无法识别未知攻击, 需提前构建攻击图
	基于溯源图	构建主机溯源图, 在图上前向和后向遍历进行检测	无法描述异常的具体信息
	结合报警与系统日志	结合溯源图分析报警信息的真实性	数据量大, 易出现路径爆炸问题, 需要研究特殊遍历算法解决数据量问题
基于混合信息	结合威胁情报与系统日志	结合威胁情报分析溯源图相似性	报警如何对应到日志中是研究难点
	结合系统日志与应用软件日志	系统日志缺乏详细细节, 使用应用软件日志为系统日志提供语义信息	需要安全专家构建威胁情报查询图, 无法识别未知威胁
	结合异构事件	异构事件建模, 多角度发现多步攻击	需要日志建模方式与关联方式研究

数据集^[134-136]、DARPA TC 数据集^[137]、DARPA OpTC^[138]数据集、DARPA GCP 数据集、NDsec^[139-141]数据集、SABU 警报共享与分析平台数据集^[142]、DEFCON CTF 数据集^[143]和自建数据集。

DARPA 2000 LLDOS 数据集由美国麻省理工学院林肯实验室于 2000 年提供, 包含 1.0^[135]和 2.0^[136]两个数据集。1.0 数据集中攻击者首先使用 ping 命令扫描寻找目标网络中存活的主机, 之后对存活主机进行 Sadmind 漏洞的探测, 使用 Sadmind 漏洞对存在漏洞的主机进行攻击, 并通过 SSH 登录受害主机, 获取 root 权限, 并下载用于进行分布式攻击的恶意木马 Mstream 和 Mstream master, 最后发起 DDos 攻击。该数据集提供了原始流量数据和有标注的 Audit 日志数据。2.0 数据集增强了攻击的隐蔽性, 通过执行 DNS HINFO 查询来探测并获取主机、平台、操作系统信息。DARPA 2000 LLDOS 数据集多用于通过流量产生报警, 对报警进行关联检测多步攻击。

DARPA TC 数据集, 是透明计算项目(DARPA Transparent Computing program)在 2019 年模拟并收集的 APT 攻击行为数据, 重点在于终端侧的攻击信息发现, 提高计算机系统的安全性。攻击过程包括可执行恶意附件、dll 侧加载、远控木马、浏览器后门等攻击模式, 涵盖 Windows、FreeBSD、Ubuntu 等多种操作系统, 包括 Audit、Dtrace、ETW 等日志类型。

溯源图相关的检测方式大多基于 DARPA 透明计算数据集。但是该数据集仅有主机日志, 不包含流量数据等信息, 因此无法实现整个网络内部的多步攻击检测。

DARPA OpTC 数据集, 是为了应对复杂的网络攻击, 尤其是 APT 攻击, DARPA 在 2021 年进一步推出的运营透明网络数据集(Operationally Trans-parent Cyber, OpTC)。该数据集收集包含 1000 个 Windows10 主机的大型网络的 6 天行为, 每台主机配有一个探测器, 以 json 格式记录主机中的事件以及流量。主机中事件以 eCAR 格式记录, 流量通过 Zeek 记录, 并且提供了主机事件与流量的映射。该数据集记录了 170 亿个事件, 其中仅 0.0016%是攻击事件。该数据集集中的类别不平衡问题与现实世界的情况一致, 给威胁检测带来了较大挑战。与 DARPA TC 数据集相比, 该数据集提供了主机事件以及网络事件, 能够更加全面地展现网络中发生的行为, 有助于检测完整的多步攻击。

DARPA GCP 数据集, 源自 DARPA 超级挑战难题(Grand Challenge Problem, GCP)项目。该数据集由 IDMEF 格式的多源报警组成, 主要用于报警关联和多步攻击检测^[43]。但是该报警数据集的获取比较困难, 目前指向数据集的链接已经失效。

NDSec 数据集是一个新型网络入侵检测数据集,

攻击形式包括自带设备办公(Bring Your Own Device, BYOD)引起的内部攻击、水坑攻击、僵尸网络等。该数据集提供了网络原始流量包和系统日志数据,并提供攻击信息标注,攻击场景也比较接近真实场景。NDSec 于 2017 年提出,目前尚未有多步攻击检测技术使用。

SABU 警报共享与分析平台数据集是 SABU 项目在 2019 年公开的报警数据集^[144]。该项目的主要目标是开发一个试点系统,以在捷克共和国的安全团队之间共享有关安全事件及其分析的信息。数据集中收集了 SABU 警报共享平台中为期一周的数据,约 1200 万条报警,以 IDEA 格式存储。

DEFCON CTF 数据集是在著名的夺旗赛(Capture The Flag, CTF)DEFCON CTF 比赛过程中收集的流量数据集。比赛采用对抗模式,每支队伍会作为防守方维护自己的服务器,阻止其他队伍攻击,同时要主动寻找并发现其他队伍服务器的漏洞,并进行攻击。目前数据集中收集了 DEFCON CTF 17 至 DEFCON CTF 26 的流量数据。因为数据来源的特殊性,数据集中大部分的流量都是真实的攻击流量,避免了攻击流量占比过小的问题,但是数据未标注,需要人工分析攻击的方式及攻击阶段。

此外,为了更好地展示所提出技术的可执行性和实验效果,部分文献使用自建数据集进行多步攻击的检测。如文献[96]设计攻击场景,在 191 台生产环境的主机上进行了为期 5 天的实验,含了 10 个真实世界的 APT 攻击,包括 Netcat 后门攻击^[145],VPNFilter 攻击^[146]等。文献[47]使用人造报警数据集进行聚类 and 报警关联的测试。这些研究使用的自建数据集一般并不开源,限制了其他研究者进行横向比较。若需要比较,则需根据描述创建相同的场景重复实验。

6.3 可能的发展方向

多步攻击检测仍是正在新兴发展的研究领域。随着攻击行为的复杂化和多样化,对发现这些攻击行为之间的逻辑关系的能力提出了更高的要求。通过对现有检测技术和数据资源的研究,我们提出了四个未来可能的研究方向。

(1)多步攻击检测的数据集研究。目前多步攻击检测的报警关联大多使用公开的 DARPA 2000 LLDOS 数据集,攻击场景较为简单,已无法匹配日益复杂的攻击行为,限制了多步攻击检测技术的测试及评估。而主机日志方面则使用 DARPA 的透明计算数据集,仅包含系统日志,无法做多维数据的综合信息。一些研究使用自建非公开数据集,无法横向

评估实验效果。多步攻击检测数据集需要做到两点:一是包含多维数据,如流量数据、系统日志数据、报警数据等;二是场景接近真实,可以考虑从 APT 报告中提取可用的攻击手段,模拟真实多步攻击。如何设计复杂的攻击场景,并保证其真实性和实用性,并包含多种数据源及标记数据是未来有意义的研究方向。

(2)基于大规模日志信息的多步攻击检测。日志详细记录系统及应用程序运行信息,但是多步攻击时间跨度可能较长,日志增长的速度快,并且攻击信息在日志中的比例很少。如何从海量日志中挖掘有效的攻击内容是多步攻击检测未来的发展方向。溯源图抽象化日志信息,通过分析图结构进行多步攻击检测,但海量日志生成的溯源图较为复杂,易出现路径爆炸问题。因此高效准确地从海量日志中挖掘多步攻击,还原攻击场景仍是需要继续研究的问题。

(3)多源信息关联的多步攻击检测。攻击线索分散于多种数据源中,如各种防护软件的报警信息、操作系统及应用软件日志、威胁情报信息等。数据源的完整且多样是多步攻击全面检测的基础,有些攻击线索只存在于某种数据源中,或者几种数据源中的攻击线索会出现重复。如何合理利用这些异构数据源,对多步攻击数据源进行建模,需要进行深入研究。未来可以结合知识图谱或态势感知进行多源数据的整合和关联。

(4)面向新型攻击方式的多步攻击检测。随着攻防博弈的深入,攻击手段在不断提升。新兴的攻击手段包括利用软件供应链攻击、无文件攻击、云环境攻击等。应对新型攻击需要评估新型攻击可能会产生的线索数据,如软件供应链攻击中恶意软件的行为方式与正常软件相比存在不同之处,可以通过比较日志发现该攻击。因此,可以对攻击产生的线索数据建模,形式化规范线索类型和内容,出现新型攻击时向模型中增加线索。另外,多步攻击具有持续性的特点,若某一环节使用了新型的攻击方式,如何通过其他攻击阶段的线索,抽丝剥茧地发现这种新型的攻击也是值得研究的问题。

7 总结

随着攻击行为的多样化和复杂化,多步攻击检测的需求越来越高。与单步攻击相比,多步攻击步骤多、时间跨度长、隐蔽性强、危害性大,相应的检测技术也有很大不同。本文对多步攻击的定义及特点做出概括,指出多步攻击检测面临的挑战,结合多

步攻击检测的发展历程, 将多步攻击检测分为基于报警信息、基于日志信息和基于混合信息三种方式, 介绍每种方式详细信息, 并进行了对比分析。随后介绍多步攻击检测研究中所用的数据集, 最后结合研究现状, 介绍多步攻击检测研究未来可能的研究方向。本文旨在为多步攻击的检测研究提供参考和启发。

参考文献

- [1] OWASP SQL Injection. https://owasp.org/www-community/attacks/SQL_Injection. Apr. 2021.
- [2] OWASP Cross Site Scripting (XSS). <https://owasp.org/www-community/attacks/xss/>. Apr. 2021.
- [3] Antonakakis M, April T, Bailey M, et al. Understanding the Mirai Botnet[C]. *The 26th USENIX Conference on Security Symposium*, 2017: 1093-1110.
- [4] Wikipedia 2016 Dyn cyberattack. https://en.wikipedia.org/wiki/2016_Dyn_cyberattack. Apr. 2021.
- [5] NIST APT Definition. <https://csre.nist.gov/glossary/term/APT>. Apr. 2021.
- [6] Cyber-Attack Against Ukrainian Critical Infrastructure. <https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01>. Apr. 2021.
- [7] CARBANAK APT THE GREAT BANK ROBBERY. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064518/Carbanak_APT_eng.pdf. Apr. 2021.
- [8] Buczak A L, Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection[J]. *IEEE Communications Surveys & Tutorials*, 2015, 18(2): 1153-1176.
- [9] Xin Y, Kong L S, Liu Z, et al. Machine Learning and Deep Learning Methods for Cybersecurity[J]. *IEEE Access*, 2018, 6: 35365-35381.
- [10] Jian S J, Lu Z G, Du D, et al. Overview of Network Intrusion Detection Technology[J]. *Journal of Cyber Security*, 2020, 5(4): 96-122.
(蹇诗婕, 卢志刚, 牡丹, 等. 网络入侵检测技术综述[J]. *信息安全学报*, 2020, 5(4): 96-122.)
- [11] Ferrag M A, Maglaras L, Moschogiannis S, et al. Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study[J]. *Journal of Information Security and Applications*, 2020, 50: 102419.
- [12] Ring M, Wunderlich S, Scheuring D, et al. A Survey of Network-Based Intrusion Detection Data Sets[J]. *Computers & Security*, 2019, 86: 147-167.
- [13] The Linux audit framework. <https://documentation.suse.com/zh-cn/sles/11-SP4/html/SLES-all/cha-audit-comp.html>. Apr. 2021.
- [14] Etw events in the common language runtime. [https://msdn.microsoft.com/en-us/library/ff357719\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/ff357719(v=vs.110).aspx). Apr. 2021.
- [15] Cyber Kill Chain. <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>. Apr. 2021.
- [16] MITRE ATT&CK. <https://attack.mitre.org/>. Apr. 2021.
- [17] Lockheed Martin. <https://www.lockheedmartin.com/en-us/index.html>. Apr. 2021.
- [18] ATT&CK Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder. <https://attack.mitre.org/techniques/T1547/001/>. Apr. 2021.
- [19] APT32. <https://attack.mitre.org/groups/G0050/>. Apr. 2021.
- [20] Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations. <https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html>. Apr. 2021.
- [21] Gao P, Xiao X S, Li Z C, et al. AIQL: Enabling Efficient Attack Investigation from System Monitoring Data[C]. *The 2018 USENIX Conference on Usenix Annual Technical Conference*, 2018: 113-125.
- [22] AIQL Multi-Step Attack Behaviors. <https://sites.google.com/site/aiqlsystem/home/attack-behaviors/multi-step-attacks>. Apr. 2021.
- [23] Trustwave Global Security Report. <https://trustwave.azureedge.net/media/13167/2015-trustwave-global-security-report.pdf>. Apr. 2021.
- [24] ATT&CK Techniques T1518. <https://attack.mitre.org/techniques/T1518/>. Apr. 2021.
- [25] Langner R. Stuxnet: Dissecting a Cyberwarfare Weapon[J]. *IEEE Security & Privacy*, 2011, 9(3): 49-51.
- [26] Lee R M, Assante M J, Conway T. Analysis of the cyber attack on the Ukrainian power grid[C]. *Electricity Information Sharing and Analysis Center*, 2016: 96-102.
- [27] Oracle and KPMG Cloud Threat Report 2020. <https://www.oracle.com/a/ocom/docs/cloud/oracle-cloud-threat-report-2020.pdf?source=ow:lp:pt::&intcmp=ow:lp:pt::Lptest>. Apr. 2021.
- [28] The Numbers Game: How Many Alerts are too Many to Handle?. <https://www.fireeye.com/offers/rpt-ide-the-numbers-game.html>. Apr. 2021.
- [29] Lee K H, Zhang X Y, Xu D Y. LogGC: Garbage Collecting Audit Log[C]. *The 2013 ACM SIGSAC conference on Computer & communications security*, 2013: 1005-1016.
- [30] Navarro J, Deruyver A, Parrend P. A Systematic Survey on Multi-Step Attack Detection[J]. *Computers & Security*, 2018, 76: 214-249.
- [31] Sadoddin R, Ghorbani A. Alert Correlation Survey: Framework and Techniques[C]. *The 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services*, 2006: 1-10.
- [32] Salah S, Maciá-Fernández G, Díaz-Verdejo J E. A Model-Based Survey of Alert Correlation Techniques[J]. *Computer Networks*, 2013, 57(5): 1289-1317.
- [33] Li Z Y, Chen Q A, Yang R Q, et al. Threat Detection and Investigation with System-Level Provenance Graphs: A Survey[J]. *Computers & Security*, 2021, 106: 102282.
- [34] Inam M A, Chen Y, Goyal A, et al. Sok: History is A Vast Early Warning System: Auditing the Provenance of System Intrusions[C]. *2023 IEEE Symposium on Security and Privacy (SP)*, 2023: 2620-2638.
- [35] IDMEF. <https://tools.ietf.org/html/rfc4765>
- [36] Ning P, Cui Y, Reeves D S, et al. Techniques and Tools for Analyzing Intrusion Alerts[J]. *ACM Transactions on Information and System Security*, 2004, 7(2): 274-318.
- [37] Li W, Tian S F. Preprocessor of Intrusion Alerts Correlation Based on Ontology[C]. *2009 WRI International Conference on Communications and Mobile Computing*, 2009: 460-464.
- [38] Ramaki A A, Khosravi-Farmad M, Bafghi A G. Real Time Alert Correlation and Prediction Using Bayesian Networks[C]. *2015*

- 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology*, 2016: 98-103.
- [39] Morin B, Mé L, Debar H, et al. M2D2: A Formal Data Model for IDS Alert Correlation[M]. *Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002: 115-137.
- [40] Taha A E, Abdel Ghaffar I, Bahaa Eldin A M, et al. Agent Based Correlation Model for Intrusion Detection Alerts[C]. *2010 IEEE International Conference on Intelligence and Security Informatics*, 2010: 89-94.
- [41] IDEA. https://idea.cesnet.cz/en/index_Apr.2021.
- [42] Lee W K, Qin X Z. Statistical Causality Analysis of Infosec Alert Data[M]. *Managing Cyber Threats*. New York: Springer-Verlag, 2005: 101-127.
- [43] Qin X Z, Lee W K. Discovering Novel Attack Strategies from INFOSEC Alerts[C]. *European Symposium on Research in Computer Security*, 2004: 439-456.
- [44] Qin X, Lee W. Attack Plan Recognition and Prediction Using Causal Networks[C]. *20th Annual Computer Security Applications Conference*, 2005: 370-379.
- [45] Soleimani M, Ghorbani A A. Multi-Layer Episode Filtering for the Multi-Step Attack Detection[J]. *Computer Communications*, 2012, 35(11): 1368-1379.
- [46] Ramaki A A, Amini M, Ebrahimi Atani R. RTECA: Real Time Episode Correlation Algorithm for Multi-Step Attack Scenarios Detection[J]. *Computers & Security*, 2015, 49: 206-219.
- [47] Haas S, Fischer M. GAC: Graph-Based Alert Correlation for the Detection of Distributed Multi-Step Attacks[C]. *The 33rd Annual ACM Symposium on Applied Computing*, 2018: 979-988.
- [48] Wang L Y, Liu A Y, Jajodia S. Using Attack Graphs for Correlating, Hypothesizing, and Predicting Intrusion Alerts[J]. *Computer Communications*, 2006, 29(15): 2917-2933.
- [49] Julisch K. Mining Alarm Clusters to Improve Alarm Handling Efficiency[C]. *Seventeenth Annual Computer Security Applications Conference*, 2002: 12-21.
- [50] Julisch K. Clustering Intrusion Detection Alarms to Support Root Cause Analysis[J]. *ACM Transactions on Information and System Security*, 6(4): 443-471.
- [51] Ban T, Samuel N, Takahashi T, et al. Combat Security Alert Fatigue with AI-assisted Techniques[C]. *Cyber Security Experimentation and Test Workshop*. 2021: 9-16.
- [52] Aminanto M E, Zhu L, Ban T, et al. Combating Threat-alert Fatigue with Online Anomaly Detection Using Isolation Forest[C]. *Neural Information Processing: 26th International Conference*, Sydney, NSW, Australia, December 12-15, 2019, Proceedings, Part I 26. Springer International Publishing, 2019: 756-765.
- [53] Van Ede T, Aghakhani H, Spahn N, et al. DeepCASE: Semi-supervised Contextual Analysis of Security Events[C]. *2022 IEEE Symposium on Security and Privacy (SP)*, 2022: 522-539.
- [54] Liu J, Zhang R, Liu W, et al. Context2Vector: Accelerating Security Event Triage via Context Representation Learning[J]. *Information and Software Technology*, 2022, 146: 106856.
- [55] Ning P, Cui Y, Reeves D S. Constructing Attack Scenarios through Correlation of Intrusion Alerts[C]. *The 9th ACM conference on Computer and communications security*, 2002: 245-254.
- [56] Ning P, Cui Y, Reeves D S. Analyzing Intensive Intrusion Alerts via Correlation[M]. *Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002: 74-94.
- [57] Ning P, Xu D B. Learning Attack Strategies from Intrusion Alerts[C]. *The 10th ACM conference on Computer and communications security*, 2003: 200-209.
- [58] Wang S, Tang G M, Kou G, et al. Attack Path Prediction Method Based on Causal Knowledge Net[J]. *Journal on Communications*, 2016, 37(10): 188-198.
(王硕, 汤光明, 寇广, 等. 基于因果知识网络的攻击路径预测方法[J]. *通信学报*, 2016, 37(10): 188-198.)
- [59] Hu Q. Attack Prediction Method Based on Multi-Step Attack Scenario[J]. *Computer Science*, 2019, 46(S1): 365-369.
(胡倩. 基于多步攻击场景的攻击预测方法[J]. *计算机科学*, 2019, 46(S1): 365-369.)
- [60] Lagzian S, Amiri F, Enayati A, et al. Frequent Item Set Mining-Based Alert Correlation for Extracting Multi-Stage Attack Scenarios[C]. *6th International Symposium on Telecommunications*, 2013: 1010-1014.
- [61] Lin T Y, Hu X H, Louie E. A Fast Association Rule Algorithm Based on Bitmap and Granular Computing[C]. *The 12th IEEE International Conference on Fuzzy Systems, 2003. FUZZ '03*, 2003: 678-683.
- [62] Zhu B, Ghorbani A A. Alert Correlation for Extracting Attack Strategies[J]. *International Journal of Network Security*, 2006, 3(3): 244-258.
- [63] Jiang J G, Wang Q W, Shi Z X, et al. The Parameter Optimization Based on LVPSO Algorithm for Detecting Multi-Step Attacks[C]. *The 16th ACM International Conference on Computing Frontiers*, 2019: 24-31.
- [64] Zhou P, Zhou G Y, Wu D K, et al. Detecting Multi-Stage Attacks Using Sequence-to-Sequence Model[J]. *Computers & Security*, 2021, 105: 102203.
- [65] Ou X M, Govindavajhala S, Appel A W. MulVAL: A Logic-Based Network Security Analyzer[C]. *The 14th conference on USENIX Security Symposium - Volume 14*, 2005: 8.
- [66] Noel S, Robertson E, Jajodia S. Correlating Intrusion Events and Building Attack Scenarios through Attack Graph Distances[C]. *20th Annual Computer Security Applications Conference*, 2005: 350-359.
- [67] Camtepe S A, Yener B. Modeling and Detection of Complex Attacks[C]. *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops - SecureComm*, 2008: 234-243.
- [68] Zhang S J, Li J H, Chen X Z, et al. Building Network Attack Graph for Alert Causal Correlation[J]. *Computers & Security*, 2008, 27(5/6): 188-196.
- [69] Chien S H, Ho C S. A Novel Threat Prediction Framework for Network Security[C]. *Advances in Information Technology and Industry Applications*, 2012: 1-9.
- [70] Du M, Li F F. Spell: Streaming Parsing of System Event Logs[C]. *2016 IEEE 16th International Conference on Data Mining*, 2017: 859-864.
- [71] Xu W, Huang L, Fox A, et al. Detecting Large-Scale System Problems by Mining Console Logs[C]. *The ACM SIGOPS 22nd symposium on Operating systems principles*, 2009: 117-132.

- [72] Beschastnikh I, Brun Y, Ernst M D, et al. Inferring Models of Concurrent Systems from Logs of Their Behavior with CSight[C]. *The 36th International Conference on Software Engineering*, 2014: 468-479.
- [73] Liu F C, Wen Y, Zhang D X, et al. Log2vec: A Heterogeneous Graph Embedding Based Approach for Detecting Cyber Threats within Enterprise[C]. *The 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019: 1777-1794.
- [74] Pei K X, Gu Z S, Saltaformaggio B, et al. HERCULE: Attack Story Reconstruction via Community Discovery on Correlated Log Graph[C]. *The 32nd Annual Conference on Computer Security Applications*, 2016: 583-595.
- [75] Liu J Y, Zhu J M, He S L, et al. Logzip: Extracting Hidden Structures via Iterative Clustering for Log Compression[C]. *2019 34th IEEE/ACM International Conference on Automated Software Engineering*, 2020: 863-873.
- [76] Du M, Li F F, Zheng G N, et al. DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning[C]. *The 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017: 1285-1298.
- [77] King S T, Chen P M. Backtracking Intrusions[C]. *The nineteenth ACM symposium on Operating systems principles*, 2003: 223-236.
- [78] Wang Q, Hassan W U, Li D, et al. You are what You Do: Hunting Stealthy Malware via Data Provenance Analysis[C]. *Proceedings 2020 Network and Distributed System Security Symposium*, 2020.
- [79] Han X, Yu X, Pasquier T, et al. SIGL: Securing Software Installations Through Deep Graph Learning[C]. *USENIX security symposium*, 2021.
- [80] Yang R Q, Ma S Q, Xu H T, et al. UISCOPE: Accurate, Instrumentation-Free, and Visible Attack Investigation for GUI Applications[C]. *Proceedings 2020 Network and Distributed System Security Symposium*, 2020.
- [81] Muniswamy-Reddy K K, Holland D A, Braun U, et al. Provenance-Aware Storage Systems[C]. *The annual conference on USENIX '06 Annual Technical Conference*, 2006: 4.
- [82] Gehani A, Tariq D. SPADE: Support for Provenance Auditing in Distributed Environments[C]. *ACM/IFIP/USENIX International Conference on Distributed Systems Platforms and Open Distributed Processing*, 2012: 101-120.
- [83] Pasquier T, Han X Y, Goldstein M, et al. Practical Whole-System Provenance Capture[C]. *The 2017 Symposium on Cloud Computing*, 2017: 405-418.
- [84] Lee K H, Zhang X, Xu D. High Accuracy Attack Provenance via Binary-based Execution Partition[C]. *Network and Distributed System Security Symposium*, 2013: Vol. 16.
- [85] Ma S, Zhai J, Wang F, et al. MPI: Multiple perspective attack investigation with semantic aware execution partitioning[C]. *26th USENIX Security Symposium*. 2017: 1111-1128.
- [86] Ma S Q, Zhang X Y, Xu D Y. ProTracer: Towards Practical Provenance Tracing by Alternating between Logging and Tainting[C]. *Proceedings 2016 Network and Distributed System Security Symposium*, 2016.
- [87] Tracepoints KERNEL. <https://www.kernel.org/doc/Documentation/trace/tracepoints.txt>. Apr. 2021.
- [88] Kwon Y, Wang F, Wang W H, et al. MCI: Modeling-Based Causality Inference in Audit Logging for Attack Investigation[C]. *Proceedings 2018 Network and Distributed System Security Symposium*, 2018.
- [89] Kwon Y, Kim D, Sumner W N, et al. LDX: Causality Inference by Lightweight Dual Execution[C]. *The Twenty-First International Conference on Architectural Support for Programming Languages and Operating Systems*, 2016: 503-515.
- [90] Xu Z, Wu Z Y, Li Z C, et al. High Fidelity Data Reduction for Big Data Security Dependency Analyses[C]. *The 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016: 504-516.
- [91] Tang Y T, Li D, Li Z C, et al. NodeMerge: Template Based Efficient Data Reduction for Big-Data Causality Analysis[C]. *The 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018: 1324-1337.
- [92] Michael N, Mink J, Liu J, et al. On the Forensic Validity of Approximated Audit Logs[C]. *ACSAC '20: Annual Computer Security Applications Conference*, 2020: 189-202.
- [93] Zeng J, Chua Z L, Chen Y F, et al. WATSON: Abstracting Behaviors from Audit Logs via Aggregation of Contextual Semantics[C]. *Proceedings 2021 Network and Distributed System Security Symposium*, 2021.
- [94] Sun X Y, Dai J, Liu P, et al. Towards Probabilistic Identification of Zero-Day Attack Paths[C]. *2016 IEEE Conference on Communications and Network Security*, 2017: 64-72.
- [95] Liu Y S, Zhang M, Li D, et al. Towards a Timely Causality Analysis for Enterprise Security[C]. *Proceedings 2018 Network and Distributed System Security Symposium*, 2018.
- [96] Hassan W U, Guo S J, Li D, et al. NoDoze: Combatting Threat Alert Fatigue with Automated Provenance Triage[C]. *Proceedings 2019 Network and Distributed System Security Symposium*, 2019.
- [97] Milajerdi S M, Gjomemo R, Eshete B, et al. HOLMES: Real-Time APT Detection through Correlation of Suspicious Information Flows[C]. *2019 IEEE Symposium on Security and Privacy*, 2019: 1137-1152.
- [98] Hassan W U, Bates A, Marino D. Tactical Provenance Analysis for Endpoint Detection and Response Systems[C]. *2020 IEEE Symposium on Security and Privacy*, 2020: 1172-1189.
- [99] Kurniawan K, Ekelhart A, Kiesling E, et al. KRYSTAL: Knowledge graph-based framework for tactical attack discovery in audit data[J]. *Computers & Security*, 2022, 121: 102828.
- [100] Han X Y, Pasquier T, Bates A, et al. Unicorn: Runtime Provenance-Based Detector for Advanced Persistent Threats[C]. *Proceedings 2020 Network and Distributed System Security Symposium*, 2020.
- [101] Hossain M N, Milajerdi S M, Wang J N, et al. SLEUTH: Real-Time Attack Scenario Reconstruction from COTS Audit Data[C]. *The 26th USENIX Conference on Security Symposium*, 2017: 487-504.
- [102] Hossain M N, Sheikh S, Sekar R. Combating Dependence Explosion in Forensic Analysis Using Alternative Tag Propagation Semantics[C]. *2020 IEEE Symposium on Security and Privacy*, 2020: 1139-1155.
- [103] King S T, Mao Z M, Lucchetti D G, et al. Enriching intrusion alerts through multi-host causality[C]. *Symposium on Network and*

- Distributed Systems Symposium*, 2005.
- [104] Zhai Y, Ning P, Xu J. Integrating IDS Alert Correlation and OS-Level Dependency Tracking[M]. *Intelligence and Security Informatics*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006: 272-284.
 - [105] Liu Y, Shu X, Sun Y, et al. RAPID: Real-Time Alert Investigation with Context-aware Prioritization for Efficient Threat Discovery[C]. *The 38th Annual Computer Security Applications Conference*. 2022: 827-840.
 - [106] Bhattarai B, Huang H. SteinerLog: prize collecting the audit logs for threat hunting on enterprise network[C]. *The 2022 ACM on Asia Conference on Computer and Communications Security*. 2022: 97-108.
 - [107] Haas S, Sommer R, Fischer M. Zeek-Osquery: Host-Network Correlation for Advanced Monitoring and Intrusion Detection[M]. *ICT Systems Security and Privacy Protection*. Cham: Springer International Publishing, 2020: 248-262.
 - [108] Zeek-osquery. <https://github.com/zeek/zeek-osquery>. Apr. 2021.
 - [109] Dhivya J, University V, Saritha A. A System for Detecting Network Intruders in Real-Time[J]. *International Journal of Computer Science and Engineering*, 2016, 3(5): 34-37.
 - [110] Osquery. <https://osquery.io/>. Apr. 2021.
 - [111] Milajerdi S M, Eshete B, Gjomemo R, et al. POIROT: Aligning Attack Behavior with Kernel Audit Records for Cyber Threat Hunting[C]. *The 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019.
 - [112] FireEye OpenIOC. <https://www.fireeye.com/blog/threat-research/2013/10/openioc-basics.html>. Apr. 2021.
 - [113] STIX. <https://stixproject.github.io/>. Apr. 2021.
 - [114] MISP. <https://www.misp-project.org/>. Apr. 2021.
 - [115] Satvat K, Gjomemo R, Venkatakrishnan V N. Extractor: Extracting attack behavior from threat reports[C]. *IEEE European Symposium on Security and Privacy (EuroS&P)*, 2021: 598-615.
 - [116] Li Z, Zeng J, Chen Y, et al. AttacKG: Constructing technique knowledge graph from cyber threat intelligence reports[C]. *European Symposium on Research in Computer Security*, 2022: 589-609.
 - [117] Hassan W U, Nouredine M A, Datta P, et al. OmegaLog: High-Fidelity Attack Investigation via Transparent Multi-Layer Log Analysis[C]. *Proceedings 2020 Network and Distributed System Security Symposium*, 2020.
 - [118] Yu L, Ma S Q, Zhang Z, et al. ALchemist: Fusing Application and Audit Logs for Precise Attack Provenance without Instrumentation[C]. *Proceedings 2021 Network and Distributed System Security Symposium*, 2021.
 - [119] Xosanavongsa C, Totel E, Bettan O. Discovering Correlations: A Formal Definition of Causal Dependency among Heterogeneous Events[C]. *2019 IEEE European Symposium on Security and Privacy*, 2019: 340-355.
 - [120] Chamotra S, Barbhuiya F A. Analysis and Modelling of Multi-Stage Attacks[C]. *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications*, 2021: 1268-1275.
 - [121] Meier M, SpringerLink. Intrusion Detection effektiv!: Modellierung und Analyse von Angriffsmustern[M]. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, 2007.
 - [122] Jaeger D, Ussath M, Cheng F, et al. Multi-Step Attack Pattern Detection on Normalized Event Logs[C]. *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing*, 2016: 390-398.
 - [123] Navarro-Lara J, Deruyver A, Parrend P. Morwilog: An ACO-Based System for Outlining Multi-Step Attacks[C]. *2016 IEEE Symposium Series on Computational Intelligence*, 2017: 1-8.
 - [124] Ussath M, Cheng F, Meinel C. Automatic Multi-Step Signature Derivation from Taint Graphs[C]. *2016 IEEE Symposium Series on Computational Intelligence*, 2017: 1-8.
 - [125] Eckmann S T, Vigna G, Kemmerer R A. STATL: An Attack Language for State-Based Intrusion Detection[J]. *Journal of Computer Security*, 2002, 10(1/2): 71-103.
 - [126] Cheung S, Lindqvist U, Fong M W. Modeling Multistep Cyber Attacks for Scenario Recognition[C]. *Proceedings DARPA Information Survivability Conference and Exposition*, 2003: 284-292.
 - [127] Event Query Language. <https://eql.readthedocs.io/en/latest/>. Apr. 2021.
 - [128] Gao P, Xiao X S, Li Z C, et al. AIQL: Enabling Efficient Attack Investigation from System Monitoring Data[C]. *The 2018 USENIX Conference on Usenix Annual Technical Conference*, 2018: 113-125.
 - [129] Gao P, Xiao X S, Li D, et al. SAQL: A Stream-Based Query System for Real-Time Abnormal System Behavior Detection[C]. *The 27th USENIX Conference on Security Symposium*, 2018: 639-656.
 - [130] 1998 DARPA Intrusion Detection Evaluation Data Set. <https://archive.ll.mit.edu/ideval/data/1998data.html>. Apr. 2021.
 - [131] 1999 DARPA Intrusion Detection Evaluation Data Set. <https://archive.ll.mit.edu/ideval/data/1999data.html>. Apr. 2021.
 - [132] Sharafaldin I, Lashkari A H, Ghorbani A A. Toward generating a new intrusion detection dataset and intrusion traffic characterization[C]. *International Conference on Information Systems Security and Privacy*. 2018: 108-116.
 - [133] KDDCUP99. <http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html>. Apr. 2021.
 - [134] DARPA 2000 Dataset. <https://www.ll.mit.edu/r-d/datasets/2000-darpa-intrusion-detection-scenario-specific-datasets>. Apr. 2021.
 - [135] DARPA 2000 Dataset 1.0. https://archive.ll.mit.edu/ideval/data/2000/LLS_DDOS_1.0.html. Apr. 2021.
 - [136] DARPA 2000 Dataset 2.0.2. https://archive.ll.mit.edu/ideval/data/2000/LLS_DDOS_2.0.2.html. Apr. 2021.
 - [137] DARPA Transparent project. <https://github.com/darpa-i2o/Transparent-Computing>. Apr. 2021.
 - [138] Anjum M M, Iqbal S, Hamelin B. Analyzing the Usefulness of the DARPA OpTC Dataset in Cyber Threat Detection Research[C]. *Proceedings of the 26th ACM Symposium on Access Control Models and Technologies*, 2021: 27-32.
 - [139] NDSec. <https://www2.hs-fulda.de/NDSec/NDSec-1/Files/>. Apr. 2021.
 - [140] Beer F, Hofer T, Karimi D, et al. A new attack composition for network security, In: Mueller P, Neumair B, Reiser H, et al. (Eds.), 10. DFN-Forum - Kommunikationstechnologien, LNI, vol. P-271, pp. 11-20, GI, Berlin, Germany, 2017.
 - [141] Beer F, Buehler U. Feature selection for flow-based intrusion detection using rough set theory, *Proceedings of the 2017 IEEE 14th*

International Conference on Networking, Sensing and Control, 2017: 617-624.

- [142] Husák M, Žádník M, Bartoš V, et al. Dataset of intrusion detection alerts from a sharing platform[J]. *Data in Brief*, 2020, 33: 106530.
- [143] DEFCON CTF. DEFCON. <https://www.defcon.org/html/links/dc-ctf.html>. Apr. 2021.
- [144] Dataset of intrusion detection alerts from a sharing platform. <https://data.mendeley.com/datasets/p6tym3fghz/1>
- [145] Persistent netcat backdoor. <https://www.offensive-security.com/metasploit-unleashed/persistent-netcat-backdoor/>, 2018. Apr. 2021.
- [146] VPNFilter: New Router Malware with Destructive Capabilities. <https://symc.ly/2IPGGVE>. Apr. 2021.



王笑语 于 2017 年在南开大学信息安全专业获得学士学位。现在中国科学院信息工程研究所攻读博士学位。研究领域为网络空间安全、线索关联。研究兴趣包括: 多步攻击检测、告警关联、溯源图技术等。Email: wangxiaoyu@iie.ac.cn



龚晓锐 于 2014 年在北京大学获得硕士学位。现任中国科学院信息工程研究所正高级工程师。研究领域为攻防对抗。研究兴趣包括移动互联网安全、网络安全攻防对抗。Email: gongxiaorui@iie.ac.cn



章秀 于 2021 年在中国科学院信息工程研究所获得博士学位。现任中国科学院信息工程研究所工程师。研究领域为渗透测试。研究兴趣包括: 攻击检测、Web 应用漏洞挖掘、渗透场景感知。Email: zhangxiu@iie.ac.cn



程子俊 于 2018 年在辽宁科技大学软件工程专业获得学士学位。现在中国科学院大学网络空间安全专业攻读博士学位。研究领域为威胁检测、告警关联、威胁溯源。研究兴趣包括: 图神经网络、图计算。Email: chengzijun@iie.ac.cn