因果图表征的网络攻击数据集构建

朱光明[1],冯家伟[2],卢梓杰[1],张向东[2],张锋军[3],牛作元[3],张　亮[1]
(1. 西安电子科技大学 计算机科学与技术学院,陕西 西安 710071;
2. 西安电子科技大学 通信工程学院,陕西 西安 710071
3. 中国电子科技集团公司第三十研究所,四川 成都 610041)

摘　要:高级可持续威胁攻击因其多阶段可持续的特性,已经成为现阶段网络攻击的主要形式。针对此类型攻击的检测、预测研究,不可避免地需要相关数据集的支撑。在构建数据集时,往往需要真实的网络与主机数据。但出于隐私与安全的考虑,很少有满足要求的开源数据集。现有的数据集也往往只提供原始的网络流和日志数据,对长时攻击上下文解析的缺乏导致单纯地利用神经网络进行数据包的恶性甄别和预测的实用性不足。为了解决这些问题,该文基于网络环境的真实攻击过程数据,构建并公布了一个基于因果图的网络攻击数据集。与传统的原始网络流和日志数据集相比,该数据集充分挖掘了攻击上下文中的因果关系,可以跨长时域对高级可持续威胁攻击进行建模,方便研究人员进行攻击检测与预测的研究。该数据集开源在 https://github.com/GuangmingZhu/CausalGraphAPTDataset 上。

关键词:网络安全;因果图;高级可持续威胁攻击;攻击上下文
中图分类号:TP391　　**文献标识码**:A　　**文章编号**:1673-629X(2024)04-0124-08
doi:10.20165/j.cnki.ISSN1673-629X.2024.0019

Network Attack Dataset Construction Using Causal Graph

ZHU Guang-ming[1],FENG Jia-wei[2],LU Zi-jie[1],ZHANG Xiang-dong[2],ZHANG Feng-jun[3],
NIU Zuo-yuan[3],ZHANG Liang[1]
(1. School of Computer Science and Technology,Xidian University,Xi'an 710071,China;
2. School of Communication Engineering,Xidian University,Xi'an 710071,China;
3. The 30th Research Institute of China Electronics Technology Group Corporation,Chengdu 610041,China)

Abstract:Advanced persistent threat attack has become the main form of network attack because of its multi-stage sustainable characteristics. Datasets are necessary for researches on the detection and prediction of this kind of attack. Real network and host data are superior when constructing datasets. However,few publicly available datasets can meet the requirements,due to the privacy and security issues. The available datasets often supply original network flows and system logs,but the absence of analysis on the long-term attack context results in that a straightforward using of deep neural networks to detect and predict malicious packets is not practical enough. In order to overcome these problems,a causal graph based network attack dataset is constructed and released,based on the real attack data of a network scene. Compared with the other datasets supplying original network flows and system logs simply,such dataset explores the causality of attach context deeply and can model the long-term advanced persistent threat attack. This makes the dataset more applicable for attack detection and prediction. The dataset is released at https://github.com/GuangmingZhu/CausalGraphAPTDataset.

Key words:network security;causal graph;advanced persistent threat attack;attack context

0　引　言

随着网络攻击技术的进步,现有的网络入侵手段不再只局限于单步攻击的执行,复杂的网络攻击通常采用多步执行的方式实施对目标系统的入侵[1]。这种高级持续性威胁(Advanced Persistent Threat,APT)攻击行为具有极强的隐蔽性和针对性,在难以察觉的情况下对目标系统造成影响极大的破坏。多年以来,APT 攻击的检测都是一个难以解决的问题,在对这个问题的研究中最重要的就是需要一个可靠的数据集来支撑对 APT 攻击过程的研究,以便于对提出的方法进行训练和测试。

网络攻击数据集中最著名的数据集是 KDD-99,

收稿日期:2023-07-13　　**修回日期**:2023-11-15
基金项目:国家重点研发计划(2020YFF0304900)
作者简介:朱光明(1987-),男,副教授,研究方向为网络安全;通信作者:张　亮(1981-),男,教授,研究方向为网络安全。

该数据集包含数百万条数据记录,包含了 4 类攻击类型,41 维数据特征包括基本特征、流量特征和内容特征[2]。随后,有研究人员提出了优化的 NSL-KDD[3],该数据集去除了原始数据集的冗余和重复记录,并保证训练集和测试集都有足够数量的数据记录,保证了良好的评估结果。UNSW-NB15[4]创建于 2015 年,由研究人员在小型仿真网络中生成的网络流量构建而成,包含了 9 种常见的网络攻击方式,从原始 PCAP 包中提取出了 41 种数据特征,共包含了 2 540 044 条数据。UNSW-NB15 存在冗余样本,这类冗余数据对于模型来说属于噪声数据,会影响模型的性能。周杰英等人[5]对此进行了数据清洗,将这些噪声数据全部删除。CICIDS2017[6] 由加拿大网络安全研究所(Canadian Institute for Cybersecurity,CIC)创建于 2017 年,在模拟环境中生成,主要由 5 天的网络流量构成。在计划的 5 天内,工作人员对实验环境实施了暴力破解、DDoS 攻击、僵尸网络、渗透攻击等多种网络攻击,对这些恶意攻击流量进行了收集并标注,正常用户行为流量则由脚本自动模拟生成。CICIDS2018[6] 于 2018 年发布,包括 7 种不同的攻击场景:暴力攻击、心血漏洞攻击、僵尸网络、DoS、DDoS、Web 攻击和网络内部的渗透;攻击基础设施包括 50 台机器,受害者组织有 5 个部门,包括 420 台机器和 30 台服务器;数据集包括每个机器的捕获网络流量和系统日志,以及使用 CICFlowMeter-V3 从捕获的流量中提取的 80 个特征。

距离现在时间较近的数据集有 DARPA OpTC[7] 和 LANL[8]。DARPA OpTC 来源于美国国防高级研究计划局(Defense Advanced Research Projects Agency,DARPA)经典数据集的多次迭代,包含了来自企业网络的 170 多亿个事件,包含持续时间为 3 天的 APT 攻击,数据集中信息的丰富性使得训练传统学习模型和深度学习模型来检测 APT 攻击或异常非常有用。但是 DARPA OpTC[9] 中恶意事件只占所有事件的 0.001 6%,良性和恶意事件之间的数量不平衡对异常和威胁检测提出了重大挑战。LANL 则是由洛斯阿拉莫斯国家实验室(Los Alamos National Laboratory,LANL)发布的统一主机和网络数据集,主机数据源于 90 天内 LANL 运行 Microsoft Windows 操作系统的大多数计算机的主机日志,网络流量数据源于 LANL 企业网络内的许多内部核心路由器,都是真实数据,但恶意行为并没有被标注。

最近,Berady 等人[10] 构建了一种新的 PWNJUTSU,通过 22 个红队来真实攻击目标系统,并通过日志系统将数据进行记录,最终得到 1 600 万条事件日志与 172 GB 的网络流量。该数据集真实的网络系统环境保证了数据的真实性,且多个红队的攻击方式和路径各有不同,保证了网络攻击的多样性。

近十年内的数据集大都开始注意 APT 攻击多阶段可持续的特性,如 CICIDS2017/2018 对渗透攻击的模拟和 DARPA OpTC 对 3 天的 APT 攻击流程的模拟。Stojanović等人[11]和 Ring 等人[12]在各自的研究中对常见的数据集做出了分析与比较,提出了现有数据集的缺陷与构建数据集的难点,包括以下几点:

(1)数据的真实性:从现实的网络中捕获的日志和流量是构建此类数据集的最佳数据源,但是因为涉及隐私和安全问题,很少有公司或机构愿意公开此类数据,所以许多团队采取了仿真环境或者合成仿真数据的方法。

(2)数据的不平衡:数据集中的攻击数据只占所有数据的极小一部分,在训练过程中,模型很难正确地学习到攻击者的攻击模式。

(3)攻击模式的单一化:真实的 APT 攻击往往包含大量的攻击方式,并通过多条攻击路径对目标系统进行攻击,然而许多数据集并不能体现这一特点。

经该文分析,常见的数据集(如表 1 所示)更多地研究网络流量中的异常,通过解析网络流量的 PCAP 包得到某些连接的数据特征,将这些数据特征作为研

表 1　数据集对比

数据集	时间	数据来源	事件总量	数据格式
KDD99[2]	1999	网络流量	约 500 万条	数据特征
NSL-KDD[3]	2009	网络流量	约 15 万条	数据特征
UNSW-NB15[4]	2015	网络流量	2 540 044 条	数据特征
CICIDS 2017[6]	2017	网络流量	2 272 894 条	PCAPs
CICIDS 2018[6]	2018	网络流量和日志文件	288 909 条	PCAPs 和数据特征
LANL[8]	2018	网络流量和系统日志	5 546 990 084 条	网络事件与主机事件
DARPA OpTC[7]	2020	网络流量和系统日志	17 433 324 390 条	eCAR 事件
PWNJUTSU[10]	2022	网络流量和系统日志	1 600 万事件与 172 GB 网络流量	Json 日志与 PCAPs
文中数据集	2023	系统日志	37 794 个节点	因果关系图

究的对象。但对于系统日志的研究同样值得注意。相较于网络流量,日志数据有以下优势:日志数据对发生的事件有更加细粒度的描述,日志数据可以更好地追踪恶意数据在主机内部的移动。近几年有很多研究工作通过系统日志来分析网络攻击事件,其中比较热门的是基于因果溯源图的分析方法,冷涛等人[13]对采用这种方法的研究工作做了综述。参考其中提到的概念方法,该文在 PWNJUTSU 的基础上,通过对主机审计日志进行解析,使用因果图表征主机的运行过程并进行攻击上下文分析,保留攻击数据记录并清除大量孤立的良性数据,构建了基于因果图的网络攻击数据集。

主要贡献有:

(1)提出一种新的日志数据处理思路,并在 PWNJUTSU 上得到验证,构建了基于因果图的网络攻击数据集。

(2)文中数据集使用因果图表征了跨多主机的 APT 攻击的上下文,有助于攻击路径重构和攻击趋势预测算法的研究。

1 数据集构建

1.1 网络环境构建

该数据集对应的网络环境将所有基础设施部署在虚拟化设备中,如图 1 所示。OPNsense 网关在互联网与目标网络间建立通信,是攻击者进行攻击的切入点。安全信息和事件管理系统(Security Information and Event Management,SIEM)负责所有日志的实时转发与索引。

目标网络共包含 3 台虚拟机,分别为 VM1、VM2 和 VM3,每台主机包含的各种服务如图 1 所示。VM1 和 VM3 使用 Linux 操作系统,VM2 使用 Windows 操作系统。3 台虚拟机只保留了与数据集构建相关的服务与账户,一些目标文件(3 台虚拟机上的多个 flag.txt 和 VM3 上的 final_flag.txt)隐藏在其主目录或者工作目录之中。攻击者被要求收集这些目标文件作为成功入侵目标网络的指标。

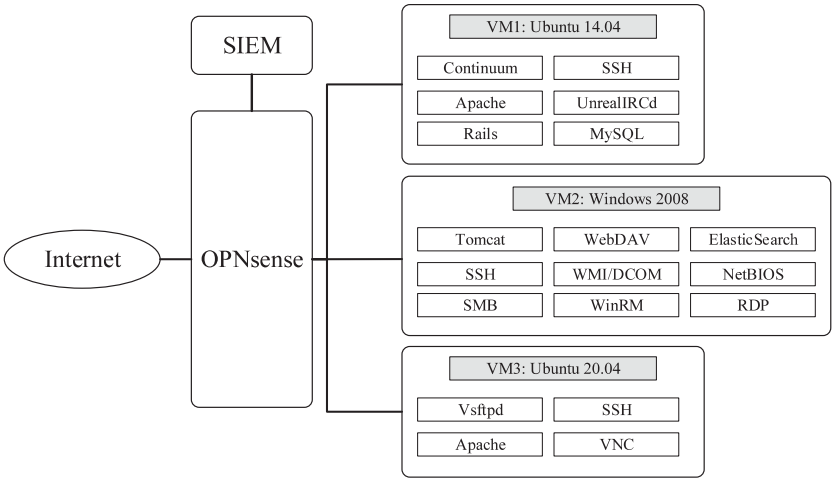

图 1 网络环境

此外,各虚拟机上安装了必要的“监测”系统,用于观察记录攻击者的行为,主要包含程序执行命令的记录、文件系统操作的记录和使用 SSH 服务的记录等。

1.2 攻击过程分析

该数据集包含 10 支红队的真实攻击行为,每支红队通过擅长的攻击技术对目标网络实施入侵。在目标网络中执行一系列的攻击战术与技术,如发现、初始访问、横向移动、权限提升等,对目标文件进行查找和收集,完成攻击任务。在具体攻击过程中,监控系统将每支红队所有的动作痕迹记录下来。

将攻击行为的每一步映射到 MITRE 定义的 ATT&CK(Adversarial Tactics,Techniques,and Common Knowledge)上,这样就可以知道攻击过程中攻击方所采用的攻击技术。大部分的攻击行为都需要在目标系统中执行特定的命令,这些动作可以很好地被日志系统捕捉到。

以数据集中某一支红队的具体攻击过程为例,该过程被分解为 18 个攻击步骤,完成了对目标网络内 3 台虚拟机的攻击,使用到了 ATT&CK 中的 8 种攻击技术。

图 2 对攻击者的攻击流程进行了详细描述。

表 2 对该攻击过程中涉及的攻击技术进行了分析,攻击方一旦在目标网络中建立立足点,后续的攻击过程基本可以通过分析不同类型的日志而解析出。尽管孤立地分析某个目标主机的日志信息无法获取到详细的攻击过程,但是综合分析攻击方在目标网络建立立足点后攻击的各个主机的日志信息,可以从中挖掘出详细的攻击过程。例如,结合横向移动的源和目的主机的日志信息,可以挖掘出横向移动过程。

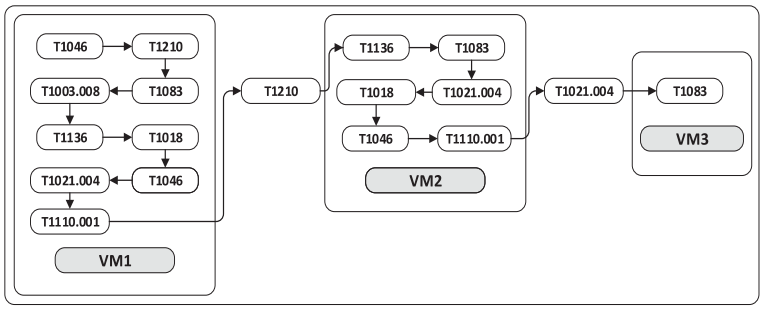

图 2　某红队的攻击流程

表 2　某红队攻击技术

攻击技术	行为描述	行为捕获
T1046	发现目标主机上的网络服务	操作日志:命令执行
T1210	利用远程服务横向移动到目标主机	服务日志:远程服务
T1083	对目标文件进行收集	操作日志:目标文件访问
T1003.008	破解/etc/passwd 和/etc/ shadow 文件获取访问凭据	操作日志:敏感文件访问
T1136	创建一个账户保证对目标主机的持续访问	操作日志:命令执行
T1018	发现可以横向移动到达的主机 IP 或主机名	操作日志:命令执行
T1110.001	对账户密码进行暴力破解	登录日志:身份验证
T1021.004	通过 SSH 远程服务登录到目标主机	服务日志:远程服务

其他红队的攻击行为与此类似,不断利用横向移动、凭证获取、权限提升、发现等战术入侵目标网络,在日志记录系统中会留下攻击痕迹。这就意味着,通过综合分析目标网络中的日志数据,可以挖掘出详细的攻击过程,包括入侵检测系统无法检测的部分攻击行为。对日志的综合解析,可以复盘重构出完整的攻击过程,进而构建相应的数据集进行攻击检测和预测算法的研究。

1.3　日志数据解析

基于上述分析,对目标网络内各主机的各类型日志进行分析,把文本类型的日志解析成因果关系图表达的数据格式,挖掘日志中各主体之间的逻辑或交互关系,表征主机运行和被攻击的详细过程。

分析 Linux 和 Windows 操作系统下的各日志类型以及表 2 中描述的攻击技术,因果关系图中节点的类型设置如下:

(1)进程节点:包括系统进程、服务进程和用户进程等。攻击者本地或远程利用进程漏洞、本地执行命令实现各战术操作,都涉及进程。从进程相关的日志中提取进程节点,解析相关操作。节点信息包括节点 ID、节点类型、进程名、主机名、进程 ID、父进程 ID、命令行、时间戳等。

(2)网络连接节点:包括主机发起或接受的网络连接,通过该节点可以捕捉跨主机攻击过程。节点信息包括节点 ID、节点类型、IP 地址、端口号、主机名、时间戳等。

(3)文件节点:包括文件、目录等,对文件的访问行为可以有效表征攻击者的持久化、凭证访问、收集、数据泄漏等战术操作。节点信息包括节点 ID、节点类型、文件名、主机名、时间戳等。

(4)登录节点:表示用户的登录行为,可以记录攻击者远程登录目标机的行为,并关联登录后攻击者执行的各类型操作。节点信息包括节点 ID、节点类型、账号名称、主机名等。

(5)注册表节点:Windows 操作系统下的各类配置信息以注册表的形式呈现,对注册表的访问也可以有效表征攻击者的持久化、凭证访问、收集、数据泄漏等战术操作。节点信息包括节点 ID、节点类型、注册表名称、主机名等。

基于上述节点定义,节点间的因果关系可以表征如表 3 所示。每个边的信息包括边 ID、边类型、主机名、时间戳等。

表 3　因果关系图中的节点和边

源节点	边(关系)	目的节点
进程节点	①进程创建	进程节点
进程节点	②进程发起网络连接	网络连接节点
网络连接节点	③进程接受网络连接	进程节点
进程节点	④进程访问文件	文件节点
进程节点	⑤进程访问注册表	注册表节点
登录节点	⑥登录创建服务进程	进程节点
网络连接节点	⑦网络连接建立	网络连接节点

基于表 3 所示的因果关系图中的节点和边,对 Linux 和 Windows 操作系统下的 auth. log、access. log、

error. log 以及各类型审计日志、服务日志等进行解析，从中挖掘出表征运行主体的节点和表征交互关系的边，构建因果关系图。

构建的原始因果关系图涵盖了各类型日志中记录的主机运行的全过程，既包含良性的正常操作，也包含被攻击的详细过程。主机的正常运行过程会产生大量的日志，进而解析出规模庞大的因果关系图，需要针对性地进行处理。具体执行的处理措施如下：

(1)删除游离节点：在解析出的原始因果关系图中存在大量的游离节点，即这些节点与其它节点之间没有连接关系，或者只与一两个节点有连接而形成孤立的微小的节点簇；这些节点无法纳入到运行上下文和攻击上下文中进行分析，需要删除以缩减因果关系图的规模。

(2)根据白名单删除良性节点：在解析出的原始因果关系图中存在大量的后台服务进程对系统文件或数据库的操作，无法区分是主机的正常服务还是攻击过程导致的，可以删除这部分节点和边以缩减因果关系图规模；另外能够判断是良性的操作的节点和边也可以根据白名单直接删除。

(3)根据黑名单标注恶性节点：根据恶意的 IP、软件、账号、文件等标注恶性的网络连接、进程、登录、文件等节点，根据因果关系标注上下文中的其它节点，形成攻击链。

根据上述方式，对 10 支红队分别执行攻击行为所产生的日志数据进行分析，最终构建基于因果关系图的网络攻击数据集，数据集统计如表 4 所示。

表 4 文中数据集统计

红队编号	日志条目总数	因果图节点数量	因果图边数量	恶性节点数量	最长攻击路径长度
1	99 200	3 442	3 170	499	9
2	81 409	1 899	1 599	174	8
3	175 204	2 094	1 864	273	11
4	215 167	4 477	4 030	614	13
5	187 113	4 626	4 006	583	13
6	106 463	2 348	2 113	180	5
7	77 188	2 140	1 900	399	9
8	407 172	5 305	4 725	1 098	15
9	426 977	6 245	5 339	190	14
10	777 701	5 218	4 606	216	12

从表 4 的统计结果可以看出：(1)构建的因果关系图中节点数目远远小于日志条目数量，并增加了表征节点间交互关系的边，提升了信息的结构化特性；(2)从不同红队的攻击过程解析出的因果关系图的节点数量以及最长攻击路径长度差异较大，体现出相同的目标网络在不同的红队攻击下所采用的战术和技术不同，这类多样性为攻击检测和预测算法研究提供了宝贵的数据支撑；(3)恶性节点在因果图节点总数中的占比在 3.0% ~20.7% 之间，避免了现有数据集恶性数据占比极少的情况，方便进行神经网络相关算法的研究。

1.4 攻击过程重建

基于解析得到的因果关系图，以恶意的 IP、软件、账号、文件等为线索，可以很容易梳理挖掘出完整的攻击过程，既包括完成攻击目标的完整攻击链，也包括探索、尝试、失败的攻击过程。以此数据集为基础，既可以进行各类型攻击检测算法的研究，也可以进行攻击预测算法的研究。下面以章节 1.2 中分析的红队攻击过程为例，从构建的因果关系图数据中对攻击过程进行重建分析。可以以对目标文件的访问为线索，逐步纵深梳理进程创建、账号登录、网络连接等一系列过程，直至检测出攻击方的 IP；再以攻击方 IP、账号等为线索，梳理重构出攻击方在目标网络的其它攻击过程，形成完整的攻击链。梳理重构出的和目标直接相关且攻击成功的攻击过程如图 3 所示，边上的序号表示在表 3 中所示的边的类型。

图 3 中只是展示了攻击链上涉及目标文件的、成功的攻击过程，实际攻击过程包含了诸多的尝试或失败的过程，并未在图 3 中完整地可视化出来。从图 3 所示的梳理重构出的攻击过程可以看出：(1)攻击方先通过社会工程学方法破解了 VM1 主机的 ssh 密码，通过远程服务入侵了 VM1 主机；接着，攻击方在 VM1 上进行信息收集，包括从/etc/shadow 和/etc/passwd 窃取账号信息，搜索发现一系列目标文件 flag. txt，通过 id 命令查询当前用户信息，通过 ping 或 nmap 命令发现目标网络内的其它主机等；此外，通过为用户 han

_solo 添加私钥,实现对 VM1 主机的持久访问。(2)攻击方在 VM1 上通过一系列的扫描探测,发现了目标主机 VM2 上的 tomcat 服务的漏洞信息,利用漏洞实现了 VM1 到 VM2 的横向移动,并建立了 VM1 和 VM2 的 C2 通信通道,并通过一系列命令获取用户和网络信息,之后添加了 gomez 用户用于实现对 VM2 主机的持久访问。(3)攻击方以 VM1 为跳板,通过 VM2 的 gomez 用户身份登录 VM2 主机,进而通过 ssh 服务横向移动到 VM3 主机,执行一系列操作实现主机信息探测及最终模板文件 final_flag. txt 的窃取。

上述重构出的攻击过程利用到了图 2 中的攻击技术,攻击过程大致与 1.2 节中红队的攻击流程相对应,而且可以直观地看出攻击者的攻击路径。总结红队的攻击过程,红队依次入侵了 VM1、VM2 和 VM3 主机,每入侵一个新的主机,都会执行一系列的操作,包括账户信息获取、权限提升、网络扫描等;一旦发现新的可入侵的主机,就会通过各种方式进行横向移动,并在下一个主机上开始新的循环。这些攻击动作都毫无例外地被日志系统所捕捉,最终通过因果图的方式展现出来。

从图 3 所示的攻击过程也可以看出,在没有任何线索的情况下,某个或某些指令的执行都和正常操作没有差异,但是当纳入到攻击上下文综合分析时,就呈现出了完整的攻击过程。该文通过上述方法,实现了对 10 个红队针对同一目标网络的不同攻击过程的分析,构建并开源了因果图表达的网络攻击数据集,用于基于攻击上下文分析的攻击检测和预测方法的研究。

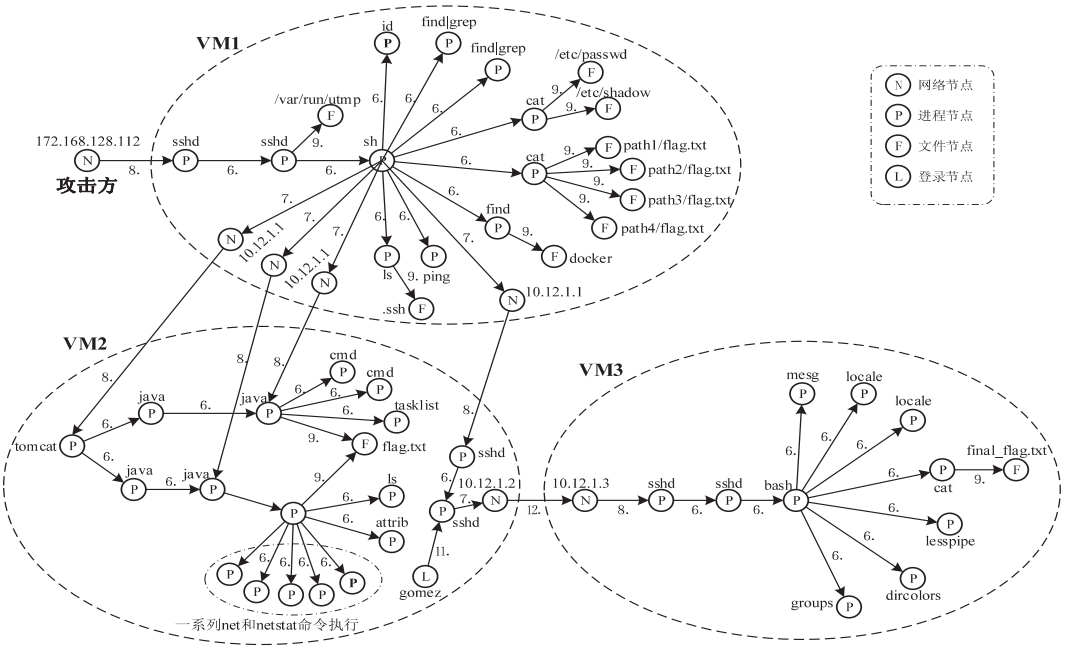

图 3　从日志中复盘出的某红队的攻击流程简略图

2　攻击趋势预测实验

2.1　数据预处理

数据集中的因果图数据并不能直接输入到模型中进行训练学习,而是需要进一步的预处理操作将数据转换为合适的格式,预处理操作主要包含攻击序列提取和数据映射。

(1)攻击序列提取:因果图数据集中包含大量的非连通的子图,每个子图包含攻击者的一次攻击操作。先删除不包含攻击上下文的子图(即子图中只包含两个节点和一条边),然后从剩余子图中分别提取以三元组形式(即<节点、边、节点>)表达的事件,把每个子图提取到的事件按时间戳排序,即可得到该子图对应的攻击序列。

(2)数据映射:节点与边的类型有限,事件是节点与边的三元组,最终得到的事件类型也是有限的,比如<进程节点、创建、进程节点>,<进程、访问、文件>等格式。将每类事件一一赋予索引值,索引与事件类型一一对应;通过 Embedding 操作将离散的数值索引映射到向量空间,得到事件向量序列作为神经网络的输入用于攻击趋势预测。

经过数据预处理后,得到的攻击序列统计如表 5 所示。

表 5　攻击序列统计

红队编号	序列数目	最大长度	最小长度	平均长度
1	10	157	4	37.8
2	7	88	3	27.1
3	12	102	3	18.8
4	10	41	3	14.5

续表 5

红队编号	序列数目	最大长度	最小长度	平均长度
5	16	72	3	18.4
6	5	117	3	37.8
7	11	108	2	26.8
8	29	152	2	21.0
9	2	26	6	16
10	13	18	2	9.2
均值	11.5	88.1	3.1	22.7

2.2 攻击预测模型

许多深度学习的模型已经被用于日志序列的检测和分析,其中应用最为广泛的是 LSTM(Long Short-Term Memory)模型[14],现已经在自然语言处理、文本生成和语音识别等领域得到广泛应用。日志条目通常遵循着严格的程序逻辑而生成,与自然语言非常类似,因此在网络安全领域中,LSTM 模型通常被用在日志序列的建模与分析工作中,比如 DeepLog 模型[15]和 DeepAG 模型[16],分别用到了 LSTM 模型及其变体 BiLSTM(Bi-directional Long Short-Term Memory)模型。BiLSTM 模型是包含两个 LSTM 模型的双向模型,可以学习来自两个方向的事件序列,分别由顺序执行的日志序列和逆序执行的日志序列所训练,最终将两个方向的预测相整合,得到更加可靠全面的结果。

该文对因果图数据集进行预处理,然后输入 DeepLog 模型和 DeepAG 模型中对日志序列进行预测,并对结果进行分析。

2.3 实验结果

将数据导入 DeepLog 和 DeepAG 模型,预测任务为接下来会发生的事件类型,分别将预测步长设置为 1,2,3。采用 10 折交叉验证方法,即 9 个红队的攻击数据用于训练,另外 1 个红队的攻击数据用于测试。为了体现在文中因果图表征的攻击上下文上进行攻击趋势预测的优势,设置了对照实验,把上文提取到的每个红队的所有攻击事件按日志顺序(即在原始日志中出现的先后顺序)排序,生成攻击序列并进行攻击趋势预测。两种攻击事件排序类型分别对应表 6 中的子图排序和日志顺序。

表 6 攻击预测精度 %

预测模型	攻击事件排序类型	预测步长	红队编号										均值
			1	2	3	4	5	6	7	8	9	10	
DeepLog[15](LSTM)	子图排序	1	77.9	71.4	61.9	71.3	87.2	78.9	82.0	84.2	70.6	84.6	77.0
		2	60.1	60.1	41.5	49.5	77.4	65.8	67.0	71.2	62.5	77.1	63.2
		3	46.7	52.1	31.8	39.2	69.9	56.2	56.5	62.1	60.0	72.7	54.7
	日志顺序	1	73.5	69.4	55.4	67.4	79.6	79.3	79.3	77.2	54.5	73.6	70.9
		2	59.3	54.2	35.7	41.8	65.5	66.3	60.9	59.3	52.4	58.7	55.4
		3	45.6	43.3	25.7	28.6	53.7	56.5	50.5	50.0	45.0	47.2	44.6
DeepAG[16](BiLSTM)	子图排序	1	76.3	71.9	62.3	71.1	87.2	79.9	82.4	84.4	77.8	86.5	78.0
		2	59.7	60.8	42.1	49.4	77.4	65.8	67.4	71.5	66.7	79.2	64.0
		3	46.7	52.9	32.5	39.2	69.9	56.2	57.0	62.4	62.5	75.0	55.4
	日志顺序	1	75.1	67.2	56.9	68.9	82.5	78.8	81.4	78.5	54.5	72.7	71.6
		2	59.1	54.2	36.1	46.3	69.4	65.7	65.8	62.1	52.4	58.7	57.0
		3	45.9	43.8	24.9	33.8	57.6	56.5	54.4	52.2	50.0	50.9	47.0

实验结果如表 6 所示。首先,按子图排序的攻击趋势预测结果全面明显优于按日志顺序的攻击趋势预测结果,这恰恰体现了使用因果图挖掘攻击上下文的优势。按原始日志顺序得到的攻击序列中会夹杂着不属于当前攻击链的攻击或非攻击过程,干扰攻击趋势的预测。另外,按子图排序的攻击趋势预测也并未取得十分巨大的领先优势,这是因为目前数据集的构建通常是构建一个专用的网络环境进行的,该环境下正常业务流不足,导致即使是在原始日志顺序上攻击过程也是相对集中的。其次,DeepAG 模型输出的测试精度比 DeepLog 模型输出的测试精度略高,这主要是因为 DeepAG 采用了效果更好的 BiLSTM 模型,更加有利于进行攻击上下信息的融合。最后,在攻击趋势的单步预测上有不错的效果,但测试精度随着预测步长的增加而减小。这是由于实验是在最细粒度的命令操作层面进行预测,而不是在战术和技术阶段层面进行预测,细粒度攻击过程的可预测性本就不足。但是,该文构建的数据集方便研究人员进一步结合攻击图和 ATT&CK 知识库,实现对下一步战术层面攻击趋势的预测;同时该数据集也方便研究人员基于攻击上下文

分析实现对攻击的检测和预测研究。

3　结束语

该文提出一种新的日志数据处理思路,并在 PWNJUTSU 上得到验证,构建了基于因果图的网络攻击数据集。构建的数据集使用因果图表征了跨多主机的 APT 攻击的上下文,有助于攻击路径重构和攻击趋势预测算法的研究,也便于研究人员结合攻击图实现下一步战术层面攻击趋势预测算法的研究。该文移植典型的 DeepLog 和 DeepAG 网络模型,在该数据集上实现了攻击趋势预测实验验证,在单步预测准确率上取得了不错的效果。在接下来的工作中,将继续完善该数据集,结合 ATT&CK 知识图谱实现多层次、多标签的数据集构建,支持广大研究人员在网络安全相关算法上的研究工作。

参考文献:

[1] 刘奇旭,王君楠,尹　捷,等. 对抗机器学习在网络入侵检测领域的应用[J]. 通信学报,2021,42(11):1-12.

[2] 刘景美,高源伯. 自适应分箱特征选择的快速网络入侵检测系统[J]. 西安电子科技大学学报,2021,48(1):176-182.

[3] TAVALLAEE M,BAGHERI E,LU W,et al. A detailed analysis of the KDD CUP 99 data set[C]//2009 IEEE symposium on computational intelligence for security and defense applications. Ottawa:IEEE,2009:53-58.

[4] MOUSTAFA N,SLAY J. UNSW-NB15:a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)[C]//2015 military communications and information systems conference (MilCIS). Canberra:IEEE,2015:1-6.

[5] 周杰英,贺鹏飞,邱荣发,等. 融合随机森林和梯度提升树的入侵检测研究[J]. 软件学报,2021,32(10):3254-3265.

[6] SHARAFALDIN I,LASHKARI A H,GHORBANI A A. Toward generating a new intrusion detection dataset and intrusion traffic characterization[C]//Proceedings of the 4th international conference on information systems security and privacy. [s. l.]:[s. n.],2018:108-116.

[7] DARPA. Operationally Transparent Cyber data release[EB/OL]. 2020. https://github. com/FiveDirections/OpTC-data.

[8] TURCOTTE M J M,KENT A D,HASH C. Unified host and network data set[M]//Data science for cyber-security. Singapore:World Scientific,2019:1-22.

[9] 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. [s. l.]:ACM,2021:27-32.

[10] BERADY A,JAUME M,TONG V V T,et al. PWNJUTSU:a dataset and a semantics-driven approach to retrace attack campaigns[J]. IEEE Transactions on Network and Service Management,2022,19(4):5252-5264.

[11] STOJANOVIĆ B,HOFER-SCHMITZ K,KLEB U. APT datasets and attack modeling for automated detection methods:a review[J]. Computers & Security,2020,92:101734.

[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] 冷　涛,蔡利君,于爱民,等. 基于系统溯源图的威胁发现与取证分析综述[J]. 通信学报,2022,43(7):172-188.

[14] HOCHREITER S,SCHMIDHUBER J. Long short-term memory[J]. Neural Computation,1997,9(8):1735-1780.

[15] DU M,LI F,ZHENG G,et al. Deeplog:anomaly detection and diagnosis from system logs through deep learning[C]//Proceedings of the 2017 ACM SIGSAC conference on computer and communications security. [s. l.]:ACM,2017:1285-1298.

[16] LI T,JIANG Y,LIN C,et al. DeepAG:attack graph construction and threats prediction with bi-directional deep learning[J]. IEEE Transactions on Dependable and Secure Computing,2022,20(1):740-757.