基于攻击链的智能渗透与攻击模拟系统

郝　伟　沈传宝　王　超　刘加勇
(北京华云安信息技术有限公司　北京　100094)
(haowei@huaun.com)

摘　要　在网络安全管理中,漏洞评估是安全评估的重要基础.然而,目前常用的漏洞评估方法仍然是以人工专家经验或基于规则的自动化脚本为主,难以适用于不断变化发展的复杂网络环境.虽然近几年人工智能技术已经取得了长足的发展,理论日趋成熟完善,但在网络安全领域智能化的高质量产品,尤其是在基于渗透测试的漏洞评估方面仍处于起步阶段.因此,为了实现渗透测试的智能化能力,华云安公司在人工智能攻防方面研究多年,设计并研发了一套基于攻击链、知识图谱和相关评估算法的智能化渗透与攻击模拟系统灵刃.对灵刃的实现原理、主要功能和应用场景进行细致的阐述说明.

关键词　漏洞评估;智能化渗透;人工智能;渗透模拟系统;产品灵刃;安全评估

中图法分类号　TP393.08

1　研究背景

漏洞评估(vulnerability assessment, VA)也称为渗透测试(penetration testing, PT),是一种对漏洞是否存在进行评估的方法,能够对漏洞进行识别和评价.经过多年的发展,漏洞评估已经是一个相对成熟的技术,但是随着互联网的快速发展、网络规模的急速扩展、用户数量的激增和各类信息的复杂性的不断提高,漏洞评估也需要与时俱进,并且这个过程充满了挑战性.在挑战和机遇中,为了进一步提升业内智能化渗透的水平,本公司研发的一套智能化渗透与攻击模拟系统灵刃,实现了具有一定智能水平的自动化漏洞评估与攻防模拟测试能力.

2　智能化渗透模拟方法

人工智能(AI)经过多年的发展,尤其是近几年的火爆,已成为一个日趋成熟的研究领域.人工智能技术的核心目标是试图让计算设备能够解决具有一定复杂性的问题.近年来,AI 在网络领域不断加深应用,如:Anderson 等人[1]尝试利用机器学习技术通过对网页头部加密的 STL 信息以及对网页是否存在恶意攻击进行分类;周仕承等人[2]通过利用强化深度学习研究如何有效发现网络的渗透弱点从而进行防御.

本公司设计和实现了虚拟化网络仿真的智能化渗透模拟系统灵刃,将公司丰富的数据资源与攻击链、智能图谱和智能化规划算法等技术进行结合.同时,考虑到 AI 应用场景的工作方式的不确定性和网络数据与 AI 所使用数据的差异,进行了大量的数据准备工作,在智能化渗透测试初期充满不确定性的前提下,为 AI 的模型建立、必要数据的准备和 AI 性能的提升打好坚实的基础.

2.1　攻击链

灵刃的核心渗透过程基于攻击链技术.攻击链也叫攻击杀伤链(attack kill chain, AKC),主要包括侦察、武器化、载荷投递、开发、安装、指挥与控制和目标行动 7 个阶段,如图 1 所示.

收稿日期:2022-08-15
引用格式:郝伟,沈传宝,王超,等. 基于攻击链的智能渗透与攻击模拟系统[J]. 信息安全研究,2022,8(增刊):60-63

图 1　基于攻击链的智能化渗透模型

阶段 1:侦察.通过各类网络目标信息采集功能,如 IP 地址探测、漏洞扫描、日志分析等,获得大量与目标相关的信息,确定目标的主要特征,为后续的渗透测试做好重要的基础准备工作.

阶段 2:武器化.对目标的渗透需要大量的攻击工具,在灵刃中包括众多常用的攻击能力(如攻击技术和工具),用于实现具体的渗透测试过程.

阶段 3:载荷投递.对攻击能力进行资源准备和部署,等待具体的任务执行.

阶段 4:漏洞利用.针对已经发现的漏洞,如 SQL 注入、XSS、RCE 等,使用已经准备好的载荷进行漏洞利用.

阶段 5:安装植入.通过对漏洞的利用,发现后门、木马和类似的恶意软件,从而实现对目标的入侵,以便实现目标的初步渗透.

阶段 6:命令与控制(command and control, C2),通过以上几个阶段的工作,最终实现对目标的命令与控制.

阶段 7:目标获取.最后攻击方通过 C2 实现了对目标的控制,从而根据实际的业务需求进行任务执行,实现作战目标,如信息获取、目标利用、目标破坏等.

2.2　知识图谱化的主体关系表示

在网络攻防过程中,需要有充分的数据作为支撑.由于在这个过程中的数据具有紧密的联系,基于图的数据表示是智能化渗透常见的表示方法,如:张继业等人[3]使用攻击图表示攻击过程;张志华[4]进一步提出了利用不同漏洞属性权重进行调整的攻击图库进行渗透测试;叶子维等人[5]在攻击图的基础上使用知识图谱进行数据的表示.因此,在灵刃中数据的表示基于知识图谱技术.

网络关系的表示方式根据不同的需求有多种表示方法,灵刃基于 Anderson 等人[1]提出的网络信息本体与关系组织方法.该模型包含了 IP、域名、资产、漏洞等主要需要关注的内容.

2.3　决策规划表示算法

在进行决策过程分析时,通过已有的知识图谱结构,基于图论的搜索方法,通过对已有关系的分析,实现攻击路径的智能决策分析.灵刃的搜索算法在原有知识图谱上,还添加了关系的权重,并利用基于 Bellman-Ford 的最短路径搜索算法 SPFA[6]来实现.SPFA 尤其适用于知识图谱的深度搜索,如段凡丁[7]提出了一种 SPFA 快速实现的优化方法.

3　产品设计

灵刃在设计过程中重点关注数据支撑能力及数据的多源开放性,从而可通过各类探针或 API 实现和其他产品的对接.灵刃的具体实现技术均采用插件式架构,在华云安丰富的数据治理经验的基础上通过使用前沿的大数据基础组件完成平台架构的构建.同时,通过由知识图谱引擎、机器学习引擎、漏洞扫描引擎、数据统计引擎、优先级计算引擎实现综合预判,使结果更加准确.

灵刃的业务层以扫描、威胁分析、知识图谱、资产管理、情报为基础搭建最符合用户需求和场景的业务组件.让系统成为用户发现漏洞的眼睛和大脑,让宏观监控、精准分析和定点处置成为现实.灵刃的功能架构如图 2 所示.

4　产品介绍

4.1　安装部署

系统分为集中式部署和分布式部署 2 种方式:

1) 集中式部署.适用于中小型网络,产品系统为二合一模式(扫描器+分析平台),若需要实现全网扫描则只需提供网络路由的相关信息即可.

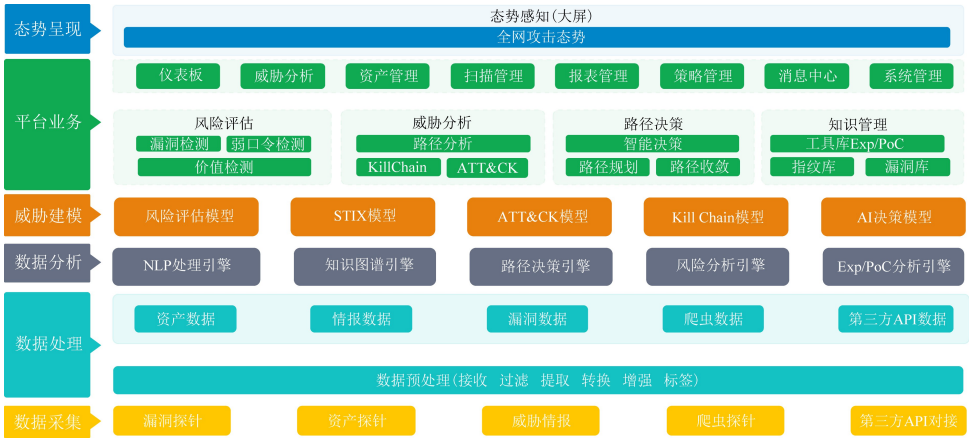

图 2　灵刃功能架构

2）分布式部署.适用大型网络，系统的扫描器和分析平台可以拆分，扫描器可下沉到各个网络域中，并将扫描结果集中上传至分析平台，并进行整体分析和呈现.

4.2　主要功能

1）信息概览.灵刃提供了丰富的全局概览信息，能够从资产、漏洞、情报、威胁等多个维度向用户展示全网整体风险情况.仪表板同时从以上纬度进行图表可视化展示，支持在不断变化的监控维度和监控重点上进行调整，并针对灵活多变的用户自定义的仪表板需求.系统提供在原有基础上新增仪表板、仪表板布局的修改以及图表大小的栅格化设定，满足用户的不同需求.

2）资产中心.灵刃提供了完整的资产管理功能，支持通过自主扫描、手动录入，情报对接，外部导入等多种方式获取资产，并通过分析引擎自动化标记未知资产、老化资产、失陷资产，帮助企业全面掌握资产的安全风险动态，协助企业彻底解决资产安全管理和安全风险跟踪的难题.

3）情报中心.灵刃支持接入多种类型的情报数据.除传统 IOC 类型数据外，还支持接入漏洞情报、数据泄露情报、代码泄露情报等扩展情报数据信息，并可将捕获到的情报信息传输给灵刃的分析引擎，使灵刃可以模拟人的渗透路径进行自动化的安全检测.为了保障情报的数据实时性和丰富性，华云安实验室有 20 余人的团队专注在数据情报的挖掘和分析中，并将进行审核标记，将情报与自身图谱模型中的数据进行关联，确保情报的真实性和可落地性，帮助用户实现动态应对外界的攻击，提前进行主动安全测试.

4）任务中心.灵刃支持多种类型的任务检测，包括资产探测、漏洞扫描、弱口令发现、智能渗透测试等.灵刃采用自研的“条件式”攻击行为触发引擎，能够将资产探测、指纹识别、PoC 验证、Exp 利用等多种安全测试行为进行统一调度，并依据各模块的上下游关系和条件约束，自主判断选择的执行工具和调用.除兼容自身多类型引擎外，灵刃还能够适配多种多款主流扫描工具和渗透工具，支持对任务及策略进行灵活配置管理.用户可根据自身需要选择灵刃中对应的策略或创建自定义策略，以实现贴合自身网络环境和业务需要的模板执行安全检测.同时，灵刃还支持按资产视角或漏洞视角，对任务执行结果进行多角度展示.

5）响应中心.灵刃本着协同优先的原则，支持用户根据自身业务灵活配置漏洞处置流程，实现了类 O2O 模式的工单流转，能够帮助企业完成漏洞全流程的处置跟踪.

6）策略管理.灵刃提供了强大的管理扫描策略，可定制自身重复使用的参数作为模板，如事先配置好要检测的端口组、插件、弱口令协议、字典等，用于实际的多人协作或统一标准化管理场景.除此以外，还可对插件的详细信息、弱口令字典库进行精细化自定义管理，如用户可根据自身网络或业务场景对插件的风险等级、漏洞描述、修复建议、标签等内容进行查看或自定义编辑，也可根据公司或私有字典库自定义弱口令典.

7）报表中心.报表是灵刃中重要的数据分析手段，高质量的报表内容能够有效地帮助用户进

行决策分析，可按照时间和空间维度持续地反馈当前网络中所存在的安全问题.系统提供 2 种类型的报表任务，分别为单次任务和周期性任务.单次任务能够立即生成报表内容，无需等待执行周期，便于汇报使用.周期性任务则会定期生成报表内容，便于从时间维度进行对比，用于辅助决策.

5 应用场景

灵刃主要适用以下 3 类攻击场景：

1）外网漏洞类场景.攻击过程首先对目标网络资产进行信息收集，获取目标的网络资产概况，对目标网络资产进行漏洞扫描，以获得漏洞情况；然后通过利用可获取系统权限的漏洞，获得外网资产系统的控制权限，通过在系统中构建网络隧道，使攻击者获取对目标内网的访问权限；接着利用横向移动攻击方式获取内网其他主机权限，并通过横向移动选择高权限的系统，控制权限下所有主机；最后通过对所控主机列表的评估和筛选，实现对高价值目标的控制和数据获取.

2）鱼叉钓鱼类场景.攻击过程首先通过收集目标外部人员信息，如邮箱、手机号、社交账号等个人属性对目标进行初步了解；然后根据其爱好、性格，攻击者对其进行定向鱼叉钓鱼，以获取其个人 PC 控制权限；最后再利用目标的主机对目标内网络等进行进一步深入渗透，以控制其网络内的更多主机.后续渗透的过程与外网漏洞类场景相同.

3）水坑钓鱼类场景.攻击过程首先设置目标群体经常访问的网站、系统等信息；然后对这类网站系统进行攻击渗透，以获得控制权限，在获得控制权限后，在已控制的网站上放置漏洞或者钓鱼水坑吸引目标群体点击，攻击访问该网站或系统的目标人员，控制目标主机，从而展开对目标人员的进一步渗透.

6 结束语

本文介绍了基于攻击链的智能化渗透和攻击模拟系统灵刃的实现原理、主要功能和应用场景.研发团队通过对多种攻击方式的全面梳理，基于智能化渗透的设计理念，使灵刃具有灵活的任务管理，并兼容多款主流扫描产品能够进行周期性的持续检测.灵刃还具备漏洞从发现到处理的全链条跟踪能力，并结合可视化显示技术呈现完整的安全趋势，从而为决策层提供了完整全面的数据支撑依据.最后，依托于公司完善的漏洞情报库及多种智能扫描策略，灵刃能够在第一时间完成重大漏洞的检测，再通过云端直接下发至用户侧，并发布对未来安全隐患的预测信息，从而帮助用户在短时间内实现情报信息的落地.

参 考 文 献

[1] Anderson B, Paul S, McGrew D. Deciphering malware's use of TLS (without decryption)[J]. Journal of Computer Virology and Hacking Techniques, 2018, 14(3): 195-211

[2] 周仕承，刘京菊，钟晓峰，等. 基于深度强化学习的智能化渗透测试路径发现[J]. 计算机科学，2021，48(7)：40-46

[3] 张继业，谢小权. 基于攻击图的渗透测试模型的设计[J]. 计算机工程与设计，2005，26(6)：1516-1519

[4] 张志华. 基于渗透测试的网络安全漏洞实时侦测技术[J]. 科学技术与工程，2018，18(20)：297-302

[5] 叶子维，郭渊博，李涛. 一种基于知识图谱的扩展攻击图生成方法[J]. 计算机科学，2019，46(12)：165-173

[6] Henzinger M R, Klein P, Rao S, Sairam Subramanian. Faster shortest-path algorithms for planar graphs [J]. Journal of Computer and System Sciences, 1997, 55(1): 3-23

[7] 段凡丁. 关于最短路径的 SPFA 快速算法[J]. 西南交通大学学报，1994，29(2)：207-212

郝 伟

博士，副研究员.主要研究方向为人工智能技术在网络安全中的应用.

haowei@huaun.com

沈传宝

硕士，国家漏洞库特聘专家.主要研究方向为国家级漏洞资源管控及共享标准、体系、机制.

shencb@huaun.com

王 超

主要研究方向为漏洞管理、实战环境下的网络攻防与攻防自动化.

wangchao@huan.com

刘加勇

主要研究方向为人工智能技术在实战环境下的自动化检测与利用.

liujy@huaun.com