基于攻击图的网络安全度量研究

赵 松[1,2], 吴晨思[2], 谢卫强[1,2], 贾紫艺[2], 王 鹤[1], 张玉清[1,2]

[1]西安电子科技大学 网络与信息安全学院 西安 中国 710071
[2]中国科学院大学 国家计算机网络入侵防范中心 北京 中国 101408

摘要 随着现代社会对网络系统依赖程度的日益增强, 网络安全问题受到普遍关注。网络安全度量是指在理解网络环境的基础之上, 建立合适指标体系和度量方法, 评估网络的安全性。本文采用攻击图这种网络脆弱性分析技术, 在对目标网络和攻击者建模的基础之上, 根据两者之间的相互关系生成攻击图模型, 分析不同的攻击路径。借鉴 CVSS 对单一漏洞的量化指标, 以及节点间概率转换关系, 提出攻击伸缩性机理。结合 CVSS 指标和攻击图, 计算攻击伸缩性数值, 并以此作为网络安全度量的方法, 最后总结了当前网络安全度量的发展现状以及面临的挑战。

关键词 攻击图模型; 安全度量; 攻击伸缩性; 安全评估
中图法分类号 TP393.1 DOI 号 10.19363/J.cnki.cn10-1380/tn.2019.01.05

Research on network security measurement based on attack graph

ZHAO Song[1,2], WU Chensi[2], XIE Weiqiang[1,2], JIA Ziyi[2], WANG He[1] , ZHANG Yuqing[1,2]

[1] School of Network and Information Security, Xidian University, Xi'an 710071, China
[2] National Computer Network Intrusion Prevention Center, University of Chinese Academy of Sciences, Beijing 101408, China

Abstract With the increasing dependence of modern society on network systems, network security issues have received widespread attention. Network security metrics are based on understanding the network environment, establishing appropriate indicator systems and metrics, and assessing network security. In this paper, using the network vulnerability analysis technology of attack graph, based on the modeling of the target network and the attacker, the attack graph model is generated based on the relationship between the two, and various possible attack paths are analyzed. This paper draws on CVSS's quantitative index of single vulnerability, and proposes the mechanism of attack scalability. Combine the CVSS indicator and the attack graph to calculate the attack scalability value and use it as a method of network security metrics. Finally, it summarizes the current development status of network security metrics and analyzes the main challenges.

Key words attack graph model; security metrics; attack scalability; security assessment

1 引言

当前, 计算机网络系统已经连接着社会的方方面面, 在带来便利的同时, 安全事件[1]的频发也造成了极大的危害。网络系统中设备普遍存在着各种安全漏洞[2], 给攻击者创造了利用设备的条件, 对网络系统埋下了隐患, 因此需要一种能够定量分析网络安全性的方法, 回答"网络系统有多安全"这个问题。

随着网络攻防技术的提升, 攻击者往往会组合利用多个漏洞进行入侵。从入侵渗透的角度, 结合网络连接关系, 网络节点情况, 脆弱性情况, 构建可能的攻击路径, 而所有攻击路径构成了攻击图。

使用攻击图模型量化评估网络安全, 是一种常见的度量方法。常见的被动检测技术, 例如入侵检测系统, 木马病毒检测, 这类检测是在攻击发生后, 根据特征匹配发现攻击。而攻击图技术需要主动发现系统中的脆弱点, 理解当前网络的安全状态。除了社会工程欺骗手段, 大部分网络攻击的发生都和漏洞相关, 攻击图是在攻击发生前的主动分析[3], 建立网络漏洞之间的关联模型, 生成攻击路径, 将得到的

通讯作者: 王鹤, 博士, 讲师, Email:wangh@nipc.org.cn。
本课题得到国家重点研发计划项目(No. 2016YFB0800700); 国家自然科学基金项目(No. 61572460, No. 61272481); 信息安全国家重点实验室的开放课题(No. 2017-ZD-01); 国家发改委信息安全专项项目［No. (2012)1424］; 国家 111 项目(No. B16037)资助。
收稿日期: 2018-09-30; 修改日期: 2018-11-27; 定稿日期: 2018-12-14

路径和指标方法结合起来, 量化分析网络安全性。

网络系统安全度量是一个复杂的问题, 更高的精确度, 意味着更高的复杂性。从技术层面到管理层面, 都可能存在脆弱点, 难以整合起来。攻击图度量方法是网络安全度量的一个子集, 网络攻击的根源是网络系统存在脆弱点, 而我们目前很难完全消除这些威胁。攻击图技术的目的在于解决这些脆弱点的关联问题, 提出一个标准的模型, 结合客观的指标度量网络安全。

攻击图的研究主要是两方面, 包括攻击图生成技术和攻击图分析技术。其中生成技术是指建立合适的模型, 整合网络系统中安全相关的数据; 分析技术是在建立的网络安全模型基础之上, 结合指标体系, 或者概率关系, 实现网络系统安全的量化评估。

本文提出了一种基于攻击图模型的网络安全度量方法, 着重分析攻击图模型的建立过程, 提出模型定义。借鉴 CVSS 指标[4], 提出攻击图节点的关联关系计算方法, 定义攻击伸缩性机理, 并以此作为度量网络安全的一种方法。

首先, 综合分析网络安全要素, 将网络系统抽象为网络拓扑图模型, 这是攻击图建立的基础[5]。拓扑图中的点表示网络主机, 边表示主机间的连接关系, 因此需要解决的问题是定义合适属性。属性值太少, 对网络系统描述不全面, 而属性值太多会造成模型复杂。本文调研大量网络架构模型和攻击图文献[6-14], 确定网络拓扑模型。

在网络拓扑的基础之上, 确定节点间的脆弱性转移关系。通过分析网络攻击以及漏洞库中信息, 确定攻击模型。这个模型表示漏洞的触发条件以及造成的影响, 结合网络拓扑图中节点连接关系, 生成攻击图模型。

攻击图模型表示的是网络中脆弱性节点的关联关系, 这些关系是攻击者可能的利用路径。网络安全度量的基本方法是计算关联概率和造成影响累积。本文从这两个角度出发, 结合指标体系, 计算了网络整体的安全状况。

本文中主要的贡献是以下两点:

1. 结合漏洞库信息, 构建攻击图模型。之前的文献对攻击模型的构建大都是参考专家知识, 定义攻击的触发条件和造成影响, 本文分析了漏洞库信息和 CVSS 漏洞评分指标, 合理的定义攻击状态的转换关系。

2. 结合 CVSS 评估指标, 计算攻击路径之间的关联关系, 提出攻击伸缩性机理以及计算方式, 作为网络安全度量的一种方法。网络安全度量分析的方法目前很少, 因为缺乏指标体系, 大部分文献采用定性分析或者定量和定性分析结合的方法。本文为定量分析网络安全提供了一个思路。

在接下来的章节中, 第 2 节介绍了攻击图的相关研究工作; 第 3 节建立网络攻击图模型, 提出攻击图生成算法; 第 4 节基于攻击图的量化分析技术, 并提出攻击伸缩性机理; 第 5 节采用实验的方式验证模型正确; 第 6 节对文章小结。

2 研究现状

攻击图的生成, 需要先对网络建模, 网络建模过程包含了大量的网络安全基础信息, 文献[15]介绍了几种常见的攻击图生成技术, 总结了基础信息包括主机配置信息、网络拓扑、漏洞信息等。目前攻击图生成方法很多, 为了便于分析, 需要研究其生成机制, 比较其中优劣。

文献[5]将攻击图分为属性攻击图和状态攻击图, 其中状态攻击图需要枚举所有的攻击路径, 存在路径爆炸问题, 现在主要的研究都是属性攻击图。综述[15]中介绍了几种主要的攻击图模型, 分别是 NetSPA、MulVAL 和 TVA。麻省理工学院提出 NetSPA (The network security planning architecture) [26,29], 使用该模型计算网络可达性, 用来表示攻击者可能利用的潜在路径。Ou 等人[28]提出了 MulVal(Multi host, multistage vulnerability analysis) 模型, 使用基于 Datalog 的网络安全分析器, 逻辑推导出节点之间的关系, 最终生成逻辑攻击图, 这种方式使用的 OVAL 漏洞描述。Noel 等人[12,18,24]提出了 TVA(Topological Vulnerability Analysis)模型, 将网络分为不同域, 其中攻击图生成使用 Ammann [9]提出的算法。随着网络规模的增大, 完全攻击图的规模变得很大, Ammann 提出单调性假设, 攻击者不会放弃已获得的高权限, 假设以最大危害程度来分析网络, 减少攻击图规模。文献[20]专门针对攻击图生成中的性能问题, 提出了分布式攻击图生成方法, 分为攻击图模型、信息采集、攻击图核心构建。其中核心部分采用平行、共享内存基础的深度优先遍历算法。

构建漏洞基础的攻击图模型, 需要与漏洞有关的攻击模板, 表示攻击的前提条件和造成的影响。以上的攻击图生成方式中, 构建的核心有所不同, 但都围绕着漏洞信息建立攻击模型。文献[13,16]专门针对了前置条件和后置状态进行了研究, 提出了一些通用的模板。文献[17]结合 NVD 漏洞库信息, 分析了自动生成攻击模板的方法。图安全模型为安全场景的分析提供了有用的方法[19], 安全场景信息包括

漏洞规格、系统访问等级、节点拓扑和可达信息。网络系统中另一重要角色是网络连接模型, 由网络拓扑和可达性组成, 这一部分包含网络访问的安全策略, 节点防御策略。从实用性出发, 好的指标具有一致性, 容易度量, 有特定的上下文环境和测量单位[1]。目前常用的有 CAPEC[23]通用攻击模式, CVSS 漏洞评分标准等。CVSS 是很有潜力的工具, 而人们对其具体内容知之甚少, 被美国国家漏洞库 NVD 等主流漏洞数据库采用, 作为漏洞评分标准。文献[14,21]使用贝叶斯网络建模网络系统中潜在的攻击路径, 基于攻击者的背景知识和攻击机制, 开发算法计算攻击路径的最优子集。建立贝叶斯攻击图, 评估风险, 其中的指标以及转移概率是参考 CVSS 值。信息安全中攻防对抗的本质可以抽象为攻防双方的策略依存性[22], 防御者所采取的防御策略是否有效, 不只取决于自身行为, 还取决于攻击者和防御系统的策略, 所以可以结合博弈论与攻击图, 研究攻防矛盾及其最优防御决策等信息安全攻防对抗难题。网络往往会遭到 0day 漏洞的攻击, 文献[25]中提出一种计算需要多少个 0day 漏洞才能破坏网络的方法, 需要越多的漏洞才能破坏, 则网络更安全。文献研究[27,30,32]基于攻击图做风险评估与安全度量, 分别提出计算网络可达性, 攻击者能力, 网络规模, 拓扑等分析方法。

基于攻击图的研究分为网络可达性分析, 构建攻击模板, 攻击图构建, 攻击图核心算法, 以及使用攻击图量化评估网络安全。攻击图生成方法已经相对成熟, 但攻击模板的构建一直以来没有很好的解决。攻击图分析方面, 主要有构建路径的指标, 结合图论算法分析。结合贝叶斯网络, 计算状态的转移概率。使用博弈论理论, 分析网络攻防之间的最优决策, 制定防御策略。

但是, 以上的研究对攻击图度量网络安全方面仍有些许不足。首先是攻击图模型的构建过程, 自动化生成攻击图一直都是难题, 因为构建攻击的状态转移关系, 大部分依旧是手工完成, 脆弱性利用条件以及造成的状态转移, 往往比较复杂。其次, 在网络安全度量方面, 常见的有风险评估模型, 忽略了不同漏洞间的关联关系, 贝叶斯方法需要大量的前提条件和假设, 生成模型复杂, 而且需要大量的先验知识。网络安全度量方面, 目前少有文献能给出具体的量化方案。

本文围绕着网络安全度量的现实需求, 以实现安全量化为目标, 在攻击图模型的基础上, 提出网络系统安全的计算方法, 为进一步研究量化评估与网络安全状态分析问题, 打下了坚实的基础。攻击图表示攻击路径, 能够更细致分析可能发生的攻击。

3 网络与攻击图模型

3.1 概述

如图 1 所示, 本文首先从网络系统物理结构分析, 定义节点和边的连接关系。然后分析主机间的连接关系, 即端口, 服务连接情况。最后将这些信息融合在一起, 实现对网络的整体认知, 构建网络拓扑图模型。这一部分是生成攻击图的基础, 而攻击图则是量化分析网络安全的基础。

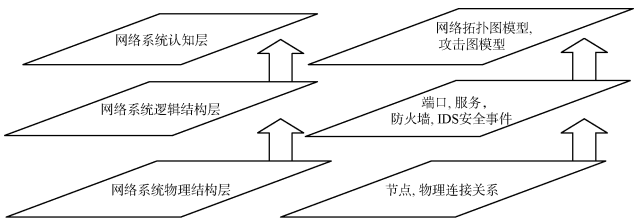

图 1 网络系统抽象模型
Figure 1 Network System Model

攻击图生成主要有两个要点:

a) 构建合适的网络拓扑模型, 指网络节点可达性信息, 节点配置以及脆弱性信息;

b) 结合漏洞库生成脆弱性转移关系, 网络攻击发生的原因是节点存在漏洞, 因此漏洞利用的条件以及造成的后果便是攻击模板。

网络度量相关信息的收集必不可少, 网络攻防是在信息及能力不对称条件下, 攻防双方的非合作博弈。网络系统安全量化分析分为三个阶段, 数据融合、数据理解和安全度量。

参考层次分析法[35], 采取从上至下, 先局部后整体的方法, 将实际网络系统按规模和层次关系, 分为系统, 主机, 服务三层。因此网络拓扑图的构建, 应该先收集主机的配置与服务作为节点信息, 并收集主机间的连接关系, 构建整个系统的图模型。

通过网络拓扑图模型构建攻击图, 需要定义合适的变量。早期的模型有些引入过多的变量, 导致模型过于复杂; 而有些模型的参数过于简单, 又不能表现一些复杂的网络攻击行为。建模的过程, 是对目标网络和攻击者的抽象描述。在网络数据的采集方面, 目前已经有了较为完善的方法和成熟的工具, 在已知的漏洞方面, 网络管理员需要比攻击者更了解网络系统脆弱性。

在下面的章节中, 为网络系统建立网络模型、攻击模型和攻击图模型。

3.2 网络拓扑图

网络拓扑结构是指网络各设备间的连接关系, 以及设备脆弱性情况, 表达了网络拓扑可达性信息, 是生成攻击图的基础。

网络拓扑图解决了网络系统中需要采集哪些关键数据信息的问题, 通过分析大量的网络系统架构和文献, 定义合适的属性:

a) 节点属性分析, 即主机节点的构成元素;

b) 边的连接分析, 即可达性分析, 是指网络之间的连接关系、防火墙的过滤规则、域划分基本安全要素分析。网络主机间的连接关系, 是攻击图状态转移的基础, 脆弱性利用的前提条件包含能否到达节点。

因此, 按照实际的网络系统结构, 作出如下定义。

定义 1: 网络拓扑图 $G=(V,E)$, 其中 $v_i \in V$, v_i 表示顶点, $e_i \in E$, e_i 表示顶点间的拓扑关系。

定义 2: 其中顶点 v 是一个七元组 $<id,ip,domain,type,vuls,sers,val>$, v 对应着网络中的实际设备, 其中, id 是节点在网络中唯一标识, ip 是节点在网络中的地址, $domain$ 是节点所属的域, $type$ 是节点类型, $vuls$ 表示节点存在的漏洞, $sers$ 表示开放的服务, val 表示节点的重要程度。

访问控制是网络安全防护的主要防护手段, 使用防火墙隔离内网, 不同主机划分在不同域。因此 domain 域信息可以表示网络攻击可能的传播状态, 可以分为 DMZ 区、核心区、内网区等。网络中设备类型主要分为主机、路由、交换机、防火墙和入侵检测设备等。$vuls$ 做为攻击者在网络间传播的主要手段, 表示节点存在的漏洞。$sers$ 表示了开放的服务, 漏洞能否利用与服务运行状态有关。

定义 3: e 是 $<sip,dip,type,pri>$, 表示网络中节点的连接关系, 其中, sip 和 dip 分别表示源主机和目的主机, $type$ 表示连接类型, pri 是访问权限。

连接关系中包含着防火墙规则, NAT 地址转换。连接类型包括域内、域间和跨域。网络系统中, 不同域之间很难相互探测到, 从攻击者角度出发, 跨域传播难度会很大。跨域类型的边在实际中是通过不同路由路径传播的。

图网络模型, 节点和边都有相应的属性。例如一台主机抽象为图中的一个节点, 则主机网络地址, 在网络中的位置信息, 开放的服务信息, 与周围主机节点连接情况, 这些基本信息作为图中边和节点的属性。抽象出节点和边的情况, 可以了解网络系统配置情况。

如图 2 所示, 一个简单网络拓扑图模型, 表示网络中边的连接关系和节点的属性值。其中节点 A 具有属性 v, 边 e1 具有属性 e, 这样就建立网络系统到图模型的转换关系, 以标准的模型反应了当前的网络状态。这个图网络模型, 能告诉管理员, 网络的具体情况, 分析属于同一局域网的节点, 也能清楚的看出存在漏洞的节点。

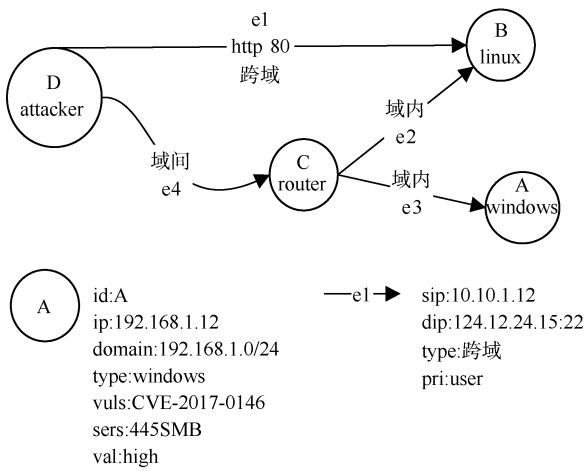

图 2 网络拓扑图模型

Figure 2 Network Topology Graph Model

3.3 攻击模板

在攻防的对抗中, 攻击者的主要突破口是网络中的脆弱点, 因此针对网络中脆弱点的利用以及其造成影响是本节一个重点。本节的主要的内容是使用前提集和后果集构建网络攻击模板。攻防信息不对称, 网络防御方能得到网络系统的信息, 预测攻击可能的发生点, 对于攻击者的能力无从得知。攻击者能通过扫描, 监听收集等方式获得目标网络的信息, 对于网络内部情况很难获取, 大部分只能是逐步的渗透测试, 不断发现网络结构。

其中前提集(Procondition)是一个状态, 表示攻击发生必要的系统环境, 如果结果为真, 则表示当前当前安全态势下, 攻击可以发生, 反之则不能发生。后果集(Postcondition)为一组状态改变的集合, 表示该类攻击发生后, 状态可能发生的改变。例如, 主机存在文件上传漏洞, 并且攻击者可以远程连接到主机, 则主机可能遭到攻击者上传木马, 节点状态改变。

为了减小攻击模型获取难度, LiWei 等[37]进行了比较深入有意义的研究, 提出了一个较为通用的攻击模型, 该模型由 3 部分组成, 分别是脆弱性实体、前提集和后果集, 如表 1 所示。

表 1 基于前提集和后果集的攻击模板

Table 1 attack template based on premise set and consequence set

攻击模型	类别	分类
脆弱性实体	操作系统 应用程序	名称 版本 体系架构 内核
前提集	访问要求 脆弱性复杂度 网络连接要求	名称 版本 源访问权限 目的访问权限 开放端口 程序
后果集	CIA 属性 网络连通关系 权限提升	机密性 完整性 可用性

结合表 1 中攻击模板内容和 NIPC 漏洞库[2,3], 定义如下, 表示网络攻击的基本模型。

定义 4: $Vul=(ID, Precondition, Postcondition)$ 攻击模型, 其中, $ID=<name,cve,cpe,cwe>$, $Precondotion=<Au,Av,Ac,Other>$, $Postcondition=<CIAimpact,private,state>$。

例如漏洞 CVE-2017-17146 是防火墙上的缓冲区溢出漏洞, 一个认证的本地攻击者通过精心构造 XML 文件, 使产品解析这个文件, 造成拒绝服务攻击或远程代码执行的后果。漏洞库关于此条记录有如下几个值:

表 2 所示, CVSS 评分字段中的 Access Vector 是访问方式, Access Complexity 是访问复杂度, Authentication 是访问权限, 这些用作 Preconception 中字段。CIA 是漏洞在机密性, 完整性可用性方面造成影响的评分, 作为 Postcondition 字段。

表 2 漏洞库字段信息

Table 2 vulnerability library field information

CVSS Base	AV:L/AC:L/Au:N/C:C/I:C/A:C
CPE	cpe:2.3:o:huawei:dp300_firmware versionsuptoincludingv500r002c00 cpe:2.3:h:huawei:dp300
CWE	Input Validation CWE-20

CPE(Common Platform Enumeration)通用平台枚举[38], 对应着脆弱性实体, 即影响设备情况。

CVE(Common Weakness Enumeration)通用弱点枚举[39], 是漏洞对应的攻击分类。

根据漏洞描述以及完整性受到的影响, 可以得出结论, Postcondition 中的状态会因为任意远程代码执行, 导致攻击者获取 root 权限, 节点转变为攻击者状态。

因此如图 3 所示, 攻击模板 *Vul*1 中, $ID=<name, CVE-201717146, CPE, CWE-20>$, $Precondition=<N, L, L, None>$, $Postcondition=(C:C/I:C/A:C$, root, attacker)。当 ID 所指向的脆弱性实体, 前提集都满足, 即值为真, 则状态发生转移, 脆弱性实体的状态转为具有 root 权限的攻击者。

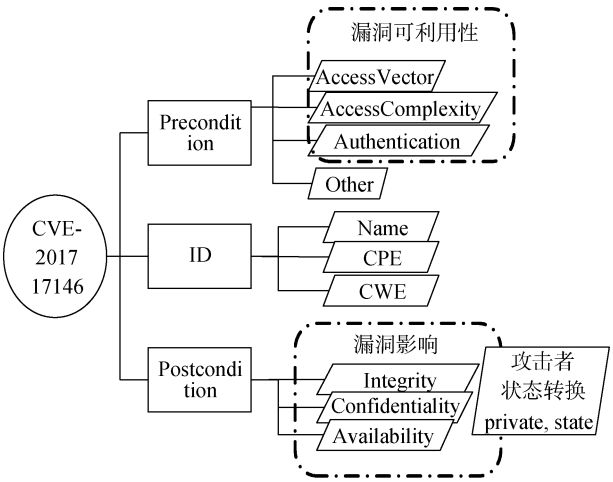

图 3 攻击模型

Figure 3 Atttack Model

为了说明完整性与攻击者状态转移的关系, 本文选取 95662 条漏洞信息, 对漏洞描述进行了词频统计, 除去文字描述中无意义的词, 统计完整性在三种状态下, 各自出现频率最高的词, 分析结果如表 3 所示。从表 3 统计分析结果可以看出, 完整性受到全部影响的漏洞, 出现频率最多的词是任意代码执行; 完整性受到部分影响的漏洞, 出现频率最多的是任意执行, 与 web 安全密切相关; 完整性没有受到影响的漏洞, 最相关的描述是拒绝服务。任意代码执行意味着攻击者已经拿到了节点管理员权限, 漏洞描述语言并不规范, 从中提取精确的状态转移比较困难, 如任意文件上传, 攻击者可以上传木马, 进一步拿到权限。因此, 可以推断出如下规则, 如果节点完整性受到影响, 则攻击者可以读/写文件, 漏洞的后置状态为攻击者获得节点权限, 可以继续感染周围节点; 如果完整性影响值为无, 则攻击者只对当前节点的机密性或可用性造成影响, 而不会转移扩散。

本节主要对漏洞攻击模型进行深入研究, 确定了标准模型, 发现了漏洞的完整性损失与攻击者状态转移之间的相关关系, 可以作为状态转移的辅助参考。

表 3 完整性与攻击者状态关系

Table 3 integrity and attacker status

完整性影响: 无	占比	完整性影响: 部分	占比	完整性影响: 全部	占比
remote	0.68	remote	0.81	arbitrary	0.58
service	0.48	arbitrary	0.62	execute	0.53
denial	0.45	php	0.46	code	0.51
information	0.22	Execute	0.34	remote	0.53
users	0.21	SQL/web/XSS	0.25	Windows	0.36

3.4 攻击图模型

本节结合网络拓扑图和攻击模板, 分析网络中攻击者可能的攻击路径, 构建攻击图模型。

攻击图模型主要分两种, 一种是状态攻击图, 一种是属性攻击图。其中状态攻击图会产生状态爆炸问题, 因此本文采用属性攻击图。属性攻击图有两类节点, 一类是漏洞利用节点, 表示一次成功的攻击; 另一类是安全状态节点, 表示节点当前状态。从状态节点指向漏洞节点的有向边, 表示攻击的前提条件; 从攻击节点指向状态节点的有向边, 表示攻击的影响后果, 即状态转换。在生成过程中, 遵循 Ammann 等提出的单调性假设, 即攻击者不会放弃已经获取的高权限。

定义 5: 攻击图 $AG=(S, A, pre, post)$, 其中 S 表示安全状态节点, A 表示漏洞利用节点, 连接关系 pre 和 $post$ 分别表示攻击的前提集和后果集。

本文模型中, 攻击图生成基于节点的可达性, 搜索在同一域内节点, 或有跨域访问节点, 传播条件是满足攻击模板。网络拓扑图中, 节点间的连接关系, 和单个漏洞节点的攻击模型状态转化关系, 使用广度优先算法[29]构建攻击图模型。

算法 1 输入为本节所定义的模型参数, 包括网络拓扑图, 攻击模板集和攻击图模型。设置初始的攻击者节点, 遍历与该节点相接的点。判断节点上存在的漏洞, 以及漏洞所对应的攻击模板。如果满足漏洞利用条件, 则将节点添加到攻击图节点中, 并添加相应的边, 最终输出攻击图模型。

算法 1. 攻击图生成算法

输入: 网络拓扑图 $G=(V,E)$ $V=<id, ip, domain, type, vuls, sers, val>$,

$E=<sip, dip, type, pri>$,

攻击集 $Vul1=(ID, Precondition, Postcondition)$,

$Precondotion=<Au, Av, Ac, Other>$,

$Postcondition=<CIAimpact, private, state>$。

攻击图 $attackerNodes=\{initial\ of\ attacker\}$

输出: 攻击图模型 $AG=(S, A, pre, post)$

过程 1.遍历网络拓扑图, 生成攻击图

```
1.  WHILE attackerNodes is not empty DO
2.    curNode = attackerNodes.pop()
3.    FOREACH v IN curNode.V.vuls DO
4.      IF curNode.state <= v.privPost
5.          curNode.state = v.privPost
6.      END
7.    END//遍历当前点上的漏洞, 确定状态
8.    destNodes = {curNode.e.dip}
9.    FOREACH dn IN destNodes DO
10.         FOREACH v2 IN dn.V.vuls DO
11.           IF v2.pre is satify AND
          dn.state <= v2.post THEN
12.                 addEdg(curNode, destNode)
13.                 attackerNode.add(dn)
14.           END
15.         END
16.       END
17.   END
```

4 网络安全量化分析

4.1 概述

攻击图是一种基于模型的网络脆弱性度量评估方法, 攻击图技术将网络中的脆弱点关联起来, 发现所有可能的攻击路径, 并且以图的方式展现出来。攻击图对网络攻击, 威胁过程的描述能力更强, 作为分析网络安全状态的一种重要方法, 为防御网络攻击, 调整网络安全策略, 改善网络安全状况提供了基础的参考。

度量空间[40], 是指具有距离函数的集合, 距离函数是指集合内所有元素间的距离, 这一距离函数称为集合上的度量, 比较直观的例子是欧式距离。因此对于网络安全度量, 参考以上定义, 结合攻击图模型, 提出计算攻击路径权重的方法, 作为度量的基本方法, 计算得出的数值即为度量标准。

本节基于 CVSS 指标和攻击图模型, 提出一种网络安全度量方法, 即攻击伸缩性计算。将攻击图中按攻击源划分为不同的攻击场景, 对于一个攻击者来说, 沿着攻击路径对系统造成损害, 形成攻击场景。攻击场景的大小, 反映了当前网络的安全状态, 即场景范围越大, 则网络越不安全, 造成的损失越多。这个场景的大小即为攻击伸缩性。

攻击伸缩性机理 *AttackScalability*: 是指攻击以

可预测的方式造成更多系统损害, 伸缩性机理是攻击造成系统损害, 预测性表现为关联情况。如式(10), 攻击伸缩性表现为攻击造成的影响与发生的概率的乘积。网络抽象为攻击图模型, 网络攻击的状态转化的根本原因是脆弱性利用, 因此, 攻击图中的攻击路径所表现的攻击者步骤, 可以理解为网络攻击伸缩性的体现。从攻击者节点出发, 到达目的节点的所有攻击路径, 构成一个攻击场景, 而所有攻击场景组成攻击图, 如图 4 所示, 图中 A, B 表示攻击图中不同的攻击场景, 攻击场景中包含着不同的攻击路径。

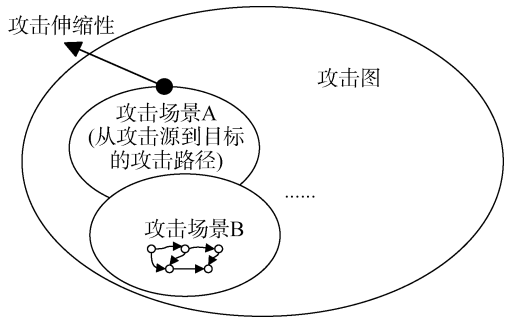

图 4 网络攻击伸缩性机理

Figure 4 network attack scalability mechanism

攻击伸缩性的计算是度量网络安全的一种方法, 从攻击者角度分析能够造成的最大危害。下面将结合 CVSS 指标, 提出攻击伸缩性计算方法, 作为网络安全的度量标准。

4.2 攻击伸缩性度量框架

如图 5(a)所示, 基础的风险评估模型由三个要素组成: 资产, 脆弱性, 威胁[8]。在完成这些要素识别之后, 给出安全指数的形式化计算, 单节点 $R = Probability * Impact$, 其中 *Risk* 表示风险值, *Probability* 表示发生的概率, *Impact* 表示造成的影响。即网络系统的安全状态由资产重要性, 威胁发生的可能性, 脆弱性造成的危害性这三点共同决定。但基础的风险评估只能给出单一资产的风险值, 对网络系统全局安全态势缺乏量化评估的能力, 忽视了脆弱性之间的关联关系。

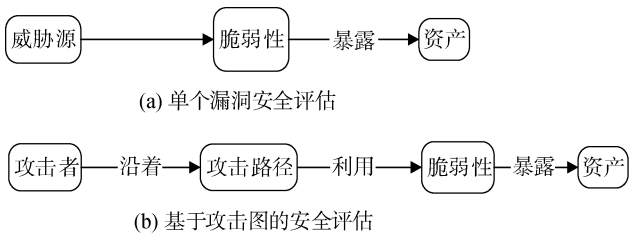

图 5 网络安全评估模型

Figure 5 Network security assessment model

基于攻击图的度量模型由四个要素组成, 额外添加了攻击路径和攻击者, 如图 5(b)。攻击图度量模型和基础风险评估模型主要区别在于, 不仅仅包括了 CVSS 的计算指标, 还添加了攻击者能力以及利用的攻击路径。其中, 攻击路径是脆弱性之间的关联关系, 是网络整体安全状态的一个体现。因此攻击图基础的度量模型, 能够量化分析多个攻击路径, 作为进一步度量全局安全态势的基础。

根据以上的度量方法分析, 本文建立如图 6 所示的总体度量框架, 首先是对网络系统信息的识别, 包括节点关联情况, 脆弱性存在情况。在此基础上生成攻击模板集, 结合网络拓扑图, 生成攻击图模型。提出路径量化评估计算方法与指标, 使用攻击伸缩性机理来说明攻击路径和攻击场景的含义, 并计算出具体的度量值, 评估网络安全状态。前面的章节已经完成了攻击图模型的建立过程, 下面的章节结合攻击图量化指标计算攻击伸缩性。

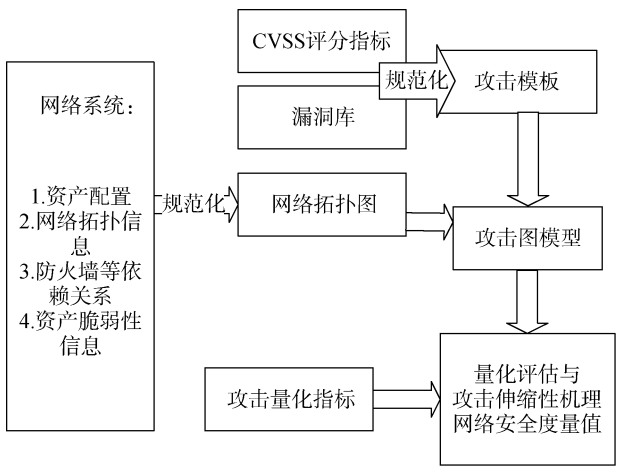

图 6 攻击伸缩性度量框架

Figure 6 attack scalability metrics framework

本文提出攻击伸缩性机理, 并以此作为度量网络安全的标准。

4.3 指标量化与计算

威胁是指可能从外部互联网或内部网络发起攻击的攻击者。在攻击图基础的模型中, 威胁主要包括两个参数: 1)利用已知漏洞对节点造成损害能力; 2)对节点发起攻击的概率。单个节点威胁计算, 是指威胁造成的影响与威胁发生的可能的乘积。

量化分析网络系统, 首先需要标准化的指标。好的指标体系需要有实用性, 能够重复分析, 容易收集, 有指定的环境信息和度量的单位。CVSS 通用漏洞评估指标, 满足以上要求, 并且被广泛认可与接受, 用于评估单个漏洞的危害性和可利用性。

CVSS 评分指标分为三个大的维度, 如图 7, 基础维度, 环境维度, 时间维度。基础维度是一个漏洞的内在特征, 分为漏洞利用和漏洞影响两部分。环境维度是主机在机密性、完整性、可用性分量上的权重。时间维度是漏洞从发现到发布完整报告, 修复补丁的, 环境维度和时间维度都是漏洞的外部环境特征。

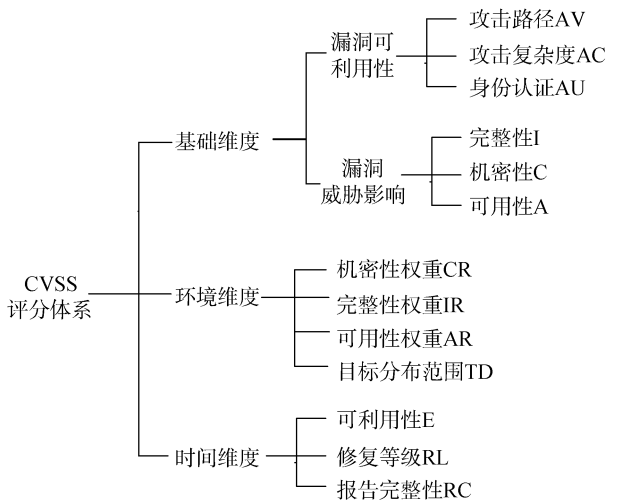

图 7 CVSS 评分指标

Figure 7 CVSS score indicator

CVSS 官方评分指标以单一漏洞为中心, 计算基础评分 BaseScore, 影响 Impact, 可利用性 Exploitability, CVSS 官网评分计算见式(1), 从式中可以看出, 单一漏洞造成的影响由机密性, 完整性, 可用性计算得到。漏洞的可利用难度, 是访问路径, 访问复杂度, 认证三方面计算得到。

$$\begin{aligned} Impact &= 10.41*\left(1-\left(1-C\right)*\left(1-I\right)*\left(1-A\right)\right) \\ Exploitability &= 20*AV*AC*AU \end{aligned} \tag{1}$$

基于攻击图攻击伸缩性计算方法与 CVSS 官方评估不同:

a) CVSS 计算方法以单个漏洞为中心, 计算单漏洞可利用性和影响。而本文是以威胁的关联分析为中心, 计算状态间的概率转移关系, 累积总的影响, 从而获得网络系统安全状态;

b) 考虑到外部环境因素的影响, 分别在评分中加入时间和环境部分指标, 并结合实际情况, 提出不同能力的攻击者指标, 威胁隐蔽指标以及节点重要程度指标。

目前大多数的评估只是对单一脆弱点的分析, 单点的安全状态计算 $R = Probability * Impact$, 即威胁发生可能与造成影响的乘积。

本节使用攻击图模型, 分析攻击路径, 将网络脆弱性关联起来, 分析整体安全状态。脆弱性之间的关联关系比脆弱性本身更重要, 因为实际中攻击者入侵渗透过程, 不会只使用单个脆弱性。攻击者为了以最小代价达成目的, 会组合利用多种不同脆弱性, 即寻找最容易的攻击路径, 达到攻击目的。

脆弱性利用之间的关联关系, 是指攻击者利用某个节点的脆弱性, 会增加相邻脆弱性节点被攻陷的概率。假设一个攻击序列由 n 个原子攻击构成, 即 $A1 \rightarrow A2 \rightarrow \ldots \rightarrow An$, 攻击 Ai 成功的概率为 Pi, $i=1,2,\ldots,n$, 则整个攻击序列的成功率可以通过式(2)计算。式(2)表示攻击序列中, 后续攻击节点受到前序攻击节点的影响。

$$P_{correlation} = \prod_{i=1}^{n} p_i \tag{2}$$

另一种形式, 攻击图节点会有多个入度的情况, 如图 8, 攻击序列的成功率通过式(3)计算。

$$P_{correlation} = 1 - \prod_{i=1}^{n} (1 - p_i) \tag{3}$$

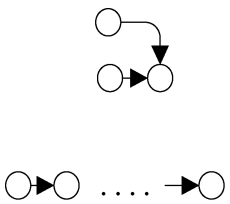

图 8 脆弱点的两种关联关系

Figure 8 two associations of vulnerabilities

如图 8 所示, 式(2)(3)两种计算形式解释了两种场景:

a) 在网络拓扑中, 如果只有单条路径, 距离攻击者越远的节点, 越难以被攻陷, 即内部节点应对威胁的能力要高于外部节点;

b) 节点的连接越多, 即图中节点入度越多, 暴露的攻击面也多, 因此增加了被攻陷的几率。

网络安全度量从整体上给出安全状态值, 不同于以往的单节点的安全分析, 需要将网络中安全漏洞关联起来。因此, 本文采用了概率的方式, 关联攻击图模型中不同节点和边。计算关联的概率之后, 累积单点威胁影响, 作为整体度量标准。所以接下工作分两部分, 一是计算节点间的关联概率, 二是计算节点的损失影响。

基于攻击图的网络安全度量, 概率计算分为两部分, 一部分是节点间的关联关系 $P_{correlation}$, 另一部分是节点自身脆弱性的利用概率 P_{inner}。P_{inner} 可以理解为, 当 $P_{correlation}=1$ 时漏洞利用的概率, 即攻击者不需要使用其他节点做为跳板, 而是直接可以连

利用到漏洞。

$$P_{inner} = Av * Ac * Au * Rc * E * Hide * Capability \quad (4)$$

式(4)中，*Av*，*Ac*，*Au* 是漏洞基础评分，表示漏洞本身的利用难度。*RC*，*E* 是漏洞生命周期评分，表示外部环境是否有详细的漏洞利用报告，漏洞的可利用性。*Hide* 和 *Capability* 是本文提出的额外指标，其中 *Hide* 是从攻击者的角度考虑攻击者的隐蔽性，威胁造成的影响越大，越容易被发现，因此 *Hide* 和漏洞影响成反比关系。*Capability* 是指攻击者能力值大小，这一部分的评判可以借助外部信息，从攻击手段判断攻击者是否是专业黑客，或者定向攻击。详细的指标值见表 4。

表 4　威胁可利用性指标

Table 4　threat availability indicator

威胁指标	指标值	数值
Av 访问向量	本地	0.40
	邻近	0.65
	网络	1
Ac 访问复杂度	高	0.35
	中	0.61
	低	0.71
Au 认证	多次	0.45
	单次	0.56
	无	0.70
RC 报告完整性	未证实	0.90
	未确认	0.95
	确认	1
	未定义	1
E 可利用性	未证实	0.85
	POC	0.90
	功能	0.95
	高	1.00
	未定义	1.00
Hide 隐蔽性	与造成的影响成反比 见表 5	
Capability 能力	范围 0.1~5(值越大能力越强)	

从威胁角度考虑网络攻击隐蔽性，节点的影响可以分为机密性 *C*，完整性 *I*，可用性 *A* 三方面，当攻击者产生网络活动，并对节点造成的影响越大，越容易被发现，因此 *Hide* 的值和 CIA 值成反比，见表 5。以攻击图为基础，节点威胁值的概率由式(5)计算，即节点被攻陷的概率由两部分组成，一部分是不同节点间的关联概率 $P_{correlation}$，另一部分是结合 CVSS 指标计算单个漏洞利用概率 P_{inner}。

$$P = P_{correlation} * P_{inner} \quad (5)$$

概率 *P* 的含义是指脆弱性利用过程中，攻击难度越大，则 *P* 值越小，节点被攻击的可能越小。

表 5　Hide 隐蔽性指标

Table 5　Hide concealment indicator

完整性	可用性影响		
	完全	部分	无
完全	0.3	0.4	0.5
部分	0.4	0.5	0.7
无	0.5	0.7	1

以上计算了节点被攻陷的概率，接下来分析脆弱性利用的影响。通过分析，威胁所能造成的影响大小，和资产的重要性密切相关，因此威胁影响计算，这一部分加入漏洞的外部环境影响，即修复等级，节点重要性定义，以及资产价值。其中修复等级是判断漏洞是否正常修复，资产价值是节点的重要性，被攻陷后，造成影响大小。网络安全评估方面，威胁对资产造成的影响，从机密性，完整性，可用性这三方面分析。

$$\text{机密性重要度 } IC = CR * C \quad (6)$$

$$\text{完整性重要度 } II = IR * I \quad (7)$$

$$\text{可用性重要度 } IA = AR * A \quad (8)$$

$$\text{威胁影响 } Impact = (IC + II + IA)/3 * RL * Val \quad (9)$$

表 6　威胁影响部分指标

Table 6　threats affect indicators

影响指标	指标值	数值
C 机密性影响	无	0.0
I 完整性影响	部分	0.275
A 可用性影响	全部	0.660
CIA 危害影响 *CR, IR, AR*	高	1.51
	中	1.0
	低	0.5
修复等级 *Remediation Level (RL)*	未定义	1.0
	官方修复	0.87
	临时修复	0.90
	变通方案	0.95
	未修复	1.00
	未定义	1.00
资产重要性 *Val*	范围 1~10(默认 1)	

攻击伸缩性计算中，P_i 由式(5)计算得到，*Impact* 由式(9)计算得到。

式(10)中攻击伸缩性是指所有节点的攻击发生概率和造成影响的累积和，其中概率 *P* 包含了节点间的关联信息。

$$AttackScalability = \sum_i P_i * Imapct_i \quad (10)$$

在攻击图中，攻击场景可以描述为从攻击源到目标所有路径集合，攻击伸缩性值是节点威胁值的累积值。*AttackScalability* 值的大小，表示网络攻击场景的安全状态，值越大，网络越不安全。

AttackScalability 的值, 反映了攻击能够造成的危害大小, 也就是当前的网络安全状态。

5 实验分析

为了验证量化度量方法的可行性和有效性, 本文搭建了如图 9 所示的小型实验环境, 其中, DMZ 区有两台服务器, 主机 1 提供邮件服务, 主机 2 提供 web 服务。信任区有三台主机, 主机 3 是用户主机, 主机 4 是管理员主机, 主机 5 是数据库主机。

如图 9 是一个实验网络系统, 包含 1 个攻击者, 5 个主机节点, 防火墙, 路由器。按照定义 1、2、3 采集网络安全信息, 图 10 是定义的网络拓扑图模型。对于节点上的漏洞信息, 从漏洞库中获取脆弱性信息, 生成攻击模板。按照算法 1 生成图 11 所示攻击图模型, 其中椭圆形代表安全状态节点, 矩形代表漏洞利用节点。

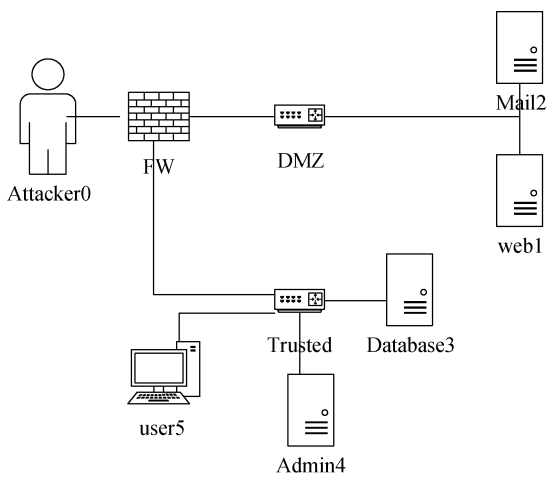

图 9 实验网络系统
Figure 9 experimental network system

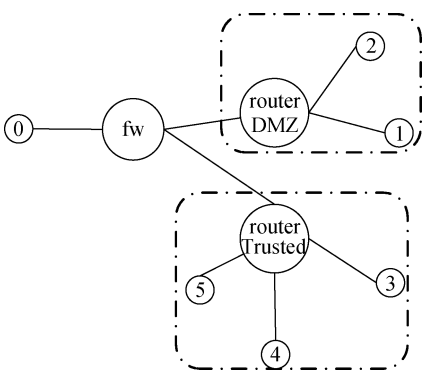

图 10 网络拓扑图
Figure 10 network topology

5.1 实验数据采集

由定义 1 采集每个节点信息 $v=<id, ip, domain, type, vuls, sers, val>$, 汇总其中的脆弱性信息, 结合防火墙配置规则提取出可能被利用的漏洞, 在漏洞库中查找到详细漏洞信息。建立节点边的连接关系, $e=<sip, dip, type, pri>$。

例如, 节点 1, $v1=<1,10.10.146.12, dmz, linux, CVE-2017-16943, Mail\ port25, high>$。

由定义 2 得到 5 个攻击模型(其中 cpe 字段太长, 未列出):

节点 1: $vul1=<<Mail, CVE-2017-16943, cpe, Use\ After\ Free(CWE-416)>, <AV:N/AC:L/Au:N, none>, <C:P/I:P/A:P, root, attacker>>$, 邮件服务器远程任意代码执行漏洞, 攻击复杂度低。

节点 2: $vul2=<<Web, CVE-2017-12615, cpe, Unrestricted\ Upload\ of\ File\ with\ Dangerous\ Type\ (CWE-434)>, <AV:N/AC:M/Au:N, none>, <C:P/I:P/A:P, root, attackers>>$, Web 远程任意文件上传漏洞。

节点 3: $vul3=<<Database, CVE-2017-16995, cpe, Buffer\ Errors\ (CWE-119)>, <AV:L/AC:L/Au:N>, <C:C/I:C/A:C, root, attacker>>$, linux 本地内核提权漏洞。

节点 4: $vul4=<<Admin, CVE-2016-0778, cpe, Buffer\ Errors(CWE-119)>, <AV:N/AC:H/Au:S, port22>\ \ <C:P/I:P/A:P, user, attacker>>$, OpenSSH 远程溢出漏洞。

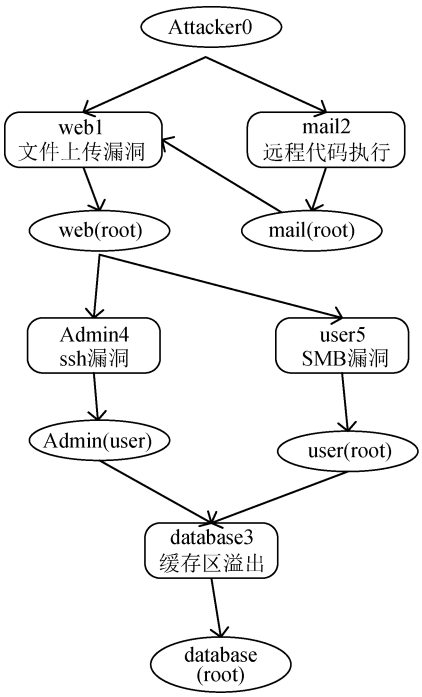

图 11 网络攻击图模型
Figure 11 Cyber attack graph model

节点 5: $vul5 = << User，CVE-2017-0146，cpe，Input\ Validation\ (CWE-20) >, < AV:N/AC:M/Au:N，port445 >, < C:C/I:C/A:C，root，attakcer >>$, Windows 上的 SMB 服务漏洞。

5.2 实验过程

1) 模型抽象

根据实验网络的具体拓扑, 安全措施以及脆弱点情况, 得到网络拓扑图, 如图 9 所示。根据攻击图生成算法, 网络拓扑图和攻击模型, 生成如图 11 所示攻击图。属性攻击图中有两类节点, 这样选择, 与状态攻击图的主要区别是不需要担心状态爆炸问题[6], 但在计算时会变的复杂。为了方便评估计算, 需要将属性攻击图进行结构转换, 如图 12 所示。因为在属性攻击图中, 状态转移和漏洞利用同时发生, 因此可以将漏洞利用节点略去, 方便计算状态转移之间的关系。

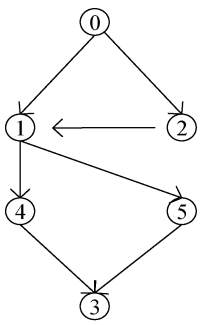

图 12 简化的攻击图结构

Figure 12 simplified attack graph structure

2) 指标选取

参考表 4、5、6 的指标量化值, 得出当前网络威胁的可用值和影响值, 见表 7。

表 7 网络威胁与影响指标值

Table 7 cyber threat and impact indicator values

	可利用性评				
	*vul*1	*vul*2	*vul*3	*vul*4	*vul*5
Av	1	1	0.4	1	1
Ac	0.71	0.61	0.71	0.35	0.61
Au	0.70	0.70	0.70	0.56	0.70
Rc	1	0.95	0.90	1	0.95
E	0.90	0.95	0.85	1	1
Hide	0.5	0.5	0.3	0.5	0.3
Capacity	2	2	2	2	2
	影响评分				
机密性	0.275	0.275	0.66	0.275	0.66
完整性	0.275	0.275	0.66	0.275	0.66
可用性	0.275	0.275	0.66	0.275	0.66
CR	0.5	1.0	1.5	0.5	0.5
IR	1.0	1.0	1.5	1.5	1.0
AR	1.5	1.5	1.0	1.0	0.5
RL	0.87	0.95	1.0	1.0	1.0
Val	4	3	10	6	1

3) 攻击伸缩性计算

首先计算单个节点的影响评分, 造成的影响由漏洞造成的危害程度以及节点重要性得出, 由式(6)(7)(8)(9)得:

$$Impact1 = 2.871$$
$$Impact2 = 2.743$$
$$Impact3 = 26.400$$
$$Impact4 = 4.950$$

计算节点脆弱性本身, 这一部分指漏洞的利用难度, 结合本文定义的指标和量化值, 由式(4)得:

$$P_{inner}(1) = 0.4473$$
$$P_{inner}(2) = 0.3854$$
$$P_{inner}(3) = 0.0912$$
$$P_{inner}(4) = 0.1960$$
$$P_{inner}(5) = 0.2434$$

计算脆弱性之前的关联关系, 计算每一个节点被攻击的概率, 由式(2)和式(3)得, 直接相连的序列, 相乘, 多个入度的节点, 计算累积概率, 依次计算出节点 1,2,3,4,5 上面脆弱性被利用可能性:

$P(0) = 1$

$P(2) = P(0)*P_{inner}(2) = 0.3854$

$P(1) = 1-(1-P(0)*P_{inner}(1))(1-P(2)*P_{inner}(1))$

$= 0.5426$

$P(4) = P(1)*P_{inner}(4) = 0.1063$

$P(5) = P(1)*P_{inner}(5) = 0.1321$

$P(3) = 1-(1-P(4)*P_{inner}(3))(1-P(5)*P_{inner}(3))$

$=0.0216$

可以看出节点威胁发生的概率符合人们常识, 即: a)外网 1, 2 节点比内网更易遭到攻击; b)节点的入度大于 1, 即更多的攻击方式, 遭到攻击的概率更大; c)序列中, 不同脆弱性利用之间相互影响。

攻击伸缩性计算, 由式(10)得:

$$AttackScalability=\sum_{i=1}^{5} P(i) * Impact(i) = 3.886$$

其中 P 是指脆弱性之间的关联关系, $Impact$ 是结合指标体系得出的脆弱性影响。

5.3 实验结果

攻击伸缩性机理定义了攻击者对网络可能造成的最大损害, 即沿着攻击路径, 对网络整体造成危害。攻击伸缩性值能够反映当前网络环境是否安全, 便于不同攻击场景之间安全程度对比。

由以上分析可以计算出当前攻击场景, 从攻击点 0 开始, 所有攻击路径造成的攻击总和, 以及单个节点威胁传播概率和威胁影响。例如, 在上述实验中, 当网络管理员修补了节点 3 上面的漏洞, 攻击伸缩值便会降低, 代表网络更加安全。相反, 攻击图中如果添加了一个节点, 则表示又有新的节点可以受到攻击者攻击, 因此攻击伸缩性值便会增大。

因此, 可以做出如下结论:

1) 攻击伸缩性机理能够以数值的方式反映当前网络安全状态, 能够客观的得出安全状态值, 符合人们的直观认识;

2) 不同攻击的伸缩性之间, 可以通过数值比较大小, 以此来比较网络的安全程度, 确定更加安全的网络系统;

3) 一个好的模型是量化评估的基础, 攻击图模型能够很好的整合网络基础信息和网络脆弱性信息, 以图模型更好的描述了网络攻击场景。良好的指标体系, 是量化评估结果客观精确的保障。

网络安全度量评估是目前网络安全研究的热点, 但目前定量的分析网络安全的研究还比较少, 下面比较了几种常见的度量评估方法, 见表 8。

表 8 量化评估方法比较

Table 8 comparison of quantitative assessment methods

模型	优点	缺点
风险评估[8]	1. 有具体的定性指标, 计算方法; 2. 操作简单, 有风险评估计算方法。	1. 只能对单个节点的脆弱性评估; 2. 专家知识定性分析, 主观性强。
贝叶斯攻击图[21]	1. 使用攻击图建立网络模型, 贝叶斯网络表示状态转移间的因果关系; 2. 结合 IDS 警报, 动态风险评估。	1. 贝叶斯推理推理中, 需要大量的先验条件和前提假设, 计算方法复杂, 随着时间的推移, 需要维护的空间较大, 实用性不强。
基于网络攻击图的安全指标[30]	1. 将指标分组到不同的“家族”中, 并组合计算单一分数; 2. 分为四组: (a. 受害者, 网络服务和漏洞; (b. 大小, 根据攻击图的大小来测量风险; (c. 包含, 按网络保护域度量; (d. 拓扑, 基于图理论, 如连接关系, 最短路径。	1. 提出的指标并没有验证有效性; 2. 只适用于特定的攻击图, 即作者自己提出的攻击图模型及生成方法。
本文	1. 以 CVSS 标准指标为基础, 并提出额外的攻击者能力, 隐蔽性, 节点重要程度等有效指标; 2. 使用攻击图模型和概率关系表示脆弱性间的关联关系; 3. 计算方法容易操作, 指标易于提取; 4. 提出攻击伸缩性机理来说明网络安全状态, 并计算出具体客观数值。	1. 缺乏度量基线, 只能做不同网络之间, 安全程度的比较。

6 小结

攻击图是网络安全状态的有效抽象, 度量方法是对网络安全的理解。

本文主要从两个方面分析:

(a. 攻击图生成技术, 网络系统需要抽象为合适的模型, 方法是定义合适的网络攻击图模型是一种主流的网络安全度量和评估方法, 本文从攻击图模型构建开始分析, 结合 CVSS 度量指标, 提出攻击伸缩性机理, 用来度量网络安全。

(b. 本文所采用的方法主要从网络攻击角度出发, 分析攻击活动的源头和类型。判断攻击者的能力, 机会,攻击成功的可能性和目的, 有效推断攻击者意图。从攻击行为和攻击目的入手, 攻击场景就是以攻击行为来推断所有的攻击者路径集合, 然后计算这些节点间的关联关系。

网络安全度量值是对整个网络的一个高层次的理解, 度量值可以用来对比安全程度, 为更好的构建安全系统提供帮助。

网络安全度量分析是一个很庞大的系统, 需要合适的指标和度量基线。度量值的精确度和网络系统的很多因素都是相关的, 例如人员管理, 实时入侵检测等。其中, 指标和度量基线是精确度量的基础。

网络安全度量需要组合考虑的指标比较多, 而单一的网络安全度量值对管理员来说, 在认识网络安全状态方面是最有利的方式。

网络安全度量计算, 主要有两个方面, 一个是节点间的概率关系, 表示节点的关联性; 另一个是累积的风险值, 作为网络总体安全状况的评估标准。

下一步工作, 将以攻击图度量安全为基础, 添加更多网络安全元素, 例如可以结合入侵检测系统的警报, 构建原子攻击的攻击链, 可以进一步扩展模型的准确性。结合安全事件, 提出更多的量化指标。结合实际情况, 精确评估漏洞被利用概率。

网络系统安全量化, 所面临的主要挑战有以下几个方面:

1. 网络数据难以全面采集, 数据的不全面, 导致对系统认识不够深入, 遗漏入侵信息;

2. 0day 漏洞的威胁, 即使网络防护固若金汤, 也可能毁于 0day, 如何评估未知漏洞和被利用率, 是网络安全度量中难题;

3. 存在很多主观因素和难以量化的部分, 例如人员管理部分, 很难用确切的数值表示。

致 谢 本课题得到国家重点研发计划“网络系统安全度量方法与指标体系”项目(No. 2016YFB0800700)资助。

参考文献

[1] A. Jaquith, “Security Metrics: Replacing Fear, Uncertainty, and Doubt,” 2007.

[2] “NIPC 国家安全漏洞库, ”http://www.nipc.org.cn/

[3] Y.Q. Zhang, S.P. Wu and Q.X. Liu, “Design and implementation of nationalsecurity vulnerability database,” *Chinese Journal on Communications*, vol.32, no.6, pp.93-100, 2011.
(张玉清, 吴舒平, 刘奇旭, 梁芳芳,“国家安全漏洞库的设计与实现”, *通信学报*, 2011,32(6): 93-100.)

[4] “Common Vulnerability Scoring System,” CVSS https://www.first.org/cvss/

[5] F. Chen, Y. Zhang, J.S. Su and W.B. Han, “Two formal analyses of attack graphs,” *Chinese Journal of Software*,” vol. 21, no. 4, pp. 838-848, 2010.
(陈锋, 张怡, 苏金树, 韩文报, “攻击图的两种形式化分析”, *软件学报*, 2010, 21(4): 838-848.)

[6] F. Chen, H.D MAO, W.M. ZHANG and C.H. LEI, ”Survey of Attack Graph Technique,”*Chinese Computer Science, vol. 38, no. 11, pp. 12-18, 2011.*
(陈锋,毛捍东,张维明,雷长海,“攻击图技术研究进展”, *计算机科学*, 2011, 38(11): 12-18.)

[7] Y. FANG, X. M. YIN and J. Z LI, “Research of quantitative network security assessment based on Bayesian-attack graphs,” *Application Research of Computers*, vol. 30, no. 9, pp. 2763-2766, 2013.
(方研, 殷肖川, 李景志,“基于贝叶斯攻击图的网络安全量化评估研究”, *计算机应用研究*, 2013, 30(9): 2763-2766.)

[8] Y. F. Wu, X.Y. Li and K. Lu,“Information Security Risk Assessment, ”China Standard Press, 2007.
(吴亚非, 李新友, 禄凯, “信息安全风险评估”, 中国标准出版社, 2007.)

[9] P. Ammann, J. Pamula and R. Ritchey, “A host-based approach to network attack chaining analysis,”*21st Annual Computer Security Applications Conference (ACSAC'05)*, pp.72-84, 2005.

[10] N. Ghosh and S. K. Ghosh, “A planner-based approach to generate and analyze minimal attack graph,” *Applied Intelligence*, vol. 36, no. 2, pp. 369-390, 2012.

[11] M. Pendleton, R. Garcia-Lebron, J. H. Cho and S. Xu, “A survey on systems security metrics,” *ACM Computing Surveys (CSUR)*, vol. 49, no. 4, pp. 62, 2017.

[12] S. Jajodia and S. Noel, “Advanced cyber attack modeling analysis and visualization,” *George Mason Univ Fairfaxva(GMUF'2011)*, pp. 1339-1344, 2011.

[13] W, Li, R.B. Vaughn and Y.S. Dandass, “An approach to model network exploitations using exploitation graphs,” *Simulation*, vol. 82, no. 8, pp. 523-541, 2006.

[14] L. Wang, T. Islam, T. Long, A. Singhal and S. Jajodia, “An attack graph-based probabilistic security metric,” *IFIP Annual Conference on Data and Applications Security and Privacy(IACDA'2008)*, pp.283-296, 2008.

[15] M.S Barik, A. Sengupta and C. Mazumdar, “Attack graph generation and analysis techniques,” *Defence Science Journal,* vol.66, no .6, pp. 559-567, 2016.

[16] G.S. Bopche and B.M. Mehtre, “Attack graph generation, visualization and analysis: Issues and challenges,” *International Symposium on Security in Computing and Communication(IACDA'2014)*, pp. 379-390, 2014.

[17] M. U. Aksu, K. Bicakci, M.H. Dilek and A.M. Ozbayoglu, “Automated Generation Of Attack Graphs Using NVD, ” *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy (PEACDASP'2018)*, pp. 135-142, 2018.

[18] S. Jajodia, S. Noel, P. Kalapa, M. Albanese and J. Williams,

"Cauldron mission-centric cyber situational awareness with defense in depth," *MILCOM*, pp. 1339-1344, 2011.

[19] B. Kordy and L. Piètre-Cambacédès, P. Schweitzer, "DAG-based attack and defense modeling: Don't miss the forest for the attack trees," *Computer Science Review*, pp. 1-38, 2014.

[20] K. Kaynar and F. Sivrikaya, "Distributed attack graph generation," *IEEE Transactions on Dependable and Secure Computing*, vol.13, no.5, pp. 519-532, 2016.

[21] N. Poolsappasit, R. Dewri and I. Ray, "Dynamic security risk management using bayesian attack graphs," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 1, pp. 61-74, 2012.

[22] W. Jiang, B.X. Fang, Z.H. Tian and H.L. Zhang, "Evaluation Network Security and Optimal Active Defend Based on Attack-Defense Game Model,"*Chinese Journal Of Computers*, vol. 32, no.4, pp. 817-827, 2009.
(姜伟, 方滨兴, 田志宏, 张宏莉, "基于攻防博弈模型的网络安全测评和最优主动防御", *计算机学报*, 2009, 32(4): 817-827.)

[23] S. Noel, "Interactive visualization and text mining for the capec cyber attack catalog," *Proceedings of the ACM Intelligent User Interfaces Workshop on Visual Text Analytics*, 2015.

[24] S. Jajodia, S. Noel and B. O'Berry, "Topological analysis of network attack vulnerability," *Managing Cyber Threats,* pp.247-266,2005.

[25] L. Wang, S. Jajodia, A. Singhal, A. Cheng, and S. noel, "k-zero day safety: A network security metric for measuring the risk of unknown vulnerabilities," *IEEE Transactions on Dependable and Secure Computing*, vol.11, no. 1, pp. 30-44, 2014.

[26] R. Lippmann, K. Ingols, C. Scott, K. Piwowarski, K. Kratkiewicz, M. Artz, and R. Cunningham, "Validating and restoring defense in depth using attack graphs," *Military Communications Conference (MCC'2006)*, pp. 1-10, 2006.

[27] L. Wang, M. Zhang, S. Jajodia S, A. Singhal, and M. Albanese, "Modeling network diversity for evaluating the robustness of networks against zero-day attacks," *European Symposium on Research in Computer Security (ESRCS'2014)*, pp. 494-511, 2014.

[28] X. Ou, S. Govindavajhala and A.W. Appel, "MulVAL: A Logic-based Network Security Analyzer," *USENIX Security Symposium (USENIX'05)*, pp. 113-128,20058.

posium (USENIX'05), pp. 113-128,20058.

[29] R. Lippmann, "Netspa: A network security planning architecture," Massachusetts Institute of Technology, 2002.

[30] S. Noel and S. Jajodia, "Metrics suite for network attack graph analytics," *Proceedings of the 9th Annual Cyber and Information Security Research Conference* (ACISRC'2014), pp. 5-8, 2014.

[31] S. Yi, Y. Peng, Q. Xiong, T. Wang, Z. Dai and L. Xu, "Overview on attack graph generation and visualization technology," *Anti-counterfeiting, security and identification (ASID'2013)*, pp. 1-6, 2013.

[32] M. Alhomidi and M. Reed, "Risk assessment and analysis through population-based attack graph modelling," *Internet Security 2013 World Congress on (WorldCIS'2013), pp.* 19-24, 2013.

[33] S. Jajodia and S. Noel, "Topological vulnerability analysis: A powerful new approach for network attack prevention, detection, and response," *Algorithms, Architectures and Information Systems Security (AAISS'2009),* pp. 285-305, 2009.

[34] X.Z. Chen, Q.H. Zheng, X.H. Guan and C.G. Lin, "Quantitative hierarchical threat evaluation model for network security," *Journal of Software*, vol. 17, no. 4, pp. 885-897, 2006.
(陈秀真, 郑庆华, 管晓宏, 林晨光, "层次化网络安全威胁态势量化评估方法", *软件学报*, 2006, 17(4): 885-897.)

[35] E.M. Hutchins, M.J. Cloppert and R.M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," *Leading Issues in Information Warfare & Security Research,* vol. 1, no. 1, pp. 113-125, 2011.

[36] W. Li, "An approach to graph-based modeling of network exploitations," Mississippi State University, 2005.

[37] "Common Platform Enumeration", CPE, http://cpe.mitre.org/about/, November, 2014

[38] "Common Weakness Enumeration", CWE, http://cwe.mitre.org/index. html, April, 2018.

[39] "Metric Space", MS, https://en.wikipedia.org/wiki/metric_space

赵松 西安电子科技大学硕士生, 主要研究方向为网络安全评估。Email: zhaos@nipc.org.cn

吴晨思 中国科学院大学博士生, 主要研究方向为信息安全与网络评估。Email: wucs@nipc.org.cn

谢卫强 西安电子科技大学硕士生, 主要研究方向为网络评估、软件安全等。Email: xiewq@nipc.org.cn

贾紫艺 中国科学院大学硕士生, 主要研究方向为网络安全、网络评估。Email: jiazy@nipc.org.cn

王鹤 博士, 讲师, 西安电子科技大学教师, 主要研究方向为量子密码协议。Email: _wangh@nipc.org.cn

张玉清 博士, 教授, 中国科学院大学博士生导师, 主要研究方向为网络与信息系统安全。Email: zhangyq@nipc.org.cn