



基于 PANAG 模型的攻击路径预测研究

王 辉, 赵 雅, 张 娟, 刘 琨

(河南理工大学 计算机科学与技术学院, 河南 焦作 454000)

摘 要: 为准确预测网络攻击路径信息, 提出一种基于概率属性网络攻击图(PANAG)的攻击路径预测方法。利用通用漏洞评分系统对弱点属性进行分析, 设计节点弱点聚类算法以减少弱点数目, 同时提出概率属性网络攻击图生成算法 GeneratNAG, 从而避免攻击图生成后可能存在的状态爆炸问题。综合分析影响网络攻击可行性的多方面因素, 引入攻击价值的概念, 提出一种基于攻击价值的路径生成算法 BuildNAP, 以消除冗余路径。在此基础上, 通过 PANAG 模型定量分析基于入侵意图的不同入侵路径的可能性, 预测攻击者最可能采取的攻击路径。实验结果表明, 该方法的准确率与执行效率均较高。

关键词: 状态变迁; 节点弱点聚类; 攻击价值; 攻击可行性; 入侵意图

开放科学(资源服务)标志码(OSID):



中文引用格式: 王辉, 赵雅, 张娟, 等. 基于 PANAG 模型的攻击路径预测研究[J]. 计算机工程, 2020, 46(9): 154-162.

英文引用格式: WANG Hui, ZHAO Ya, ZHANG Juan, et al. Research on attack path prediction based on PANAG model[J]. Computer Engineering, 2020, 46(9): 154-162.

Research on Attack Path Prediction Based on PANAG Model

WANG Hui, ZHAO Ya, ZHANG Juan, LIU Kun

(College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo, Henan 454000, China)

[Abstract] In order to accurately predict network attack paths, this paper proposes an attack path prediction method based on Probabilistic Attribute Network Attack Graph(PANAG). The method uses the common vulnerability scoring system to analyze the vulnerability attributes, and designs a Node Vulnerability Clustering(NVC) algorithm to reduce the number of vulnerabilities. Also, the probability attribute network attack graph generation algorithm, GeneratNAG, is given to avoid the possible state explosion of generated attack graphs. Then a comprehensive analysis of factors that influence the feasibility of cyberattacks is made, and on this basis the concept of attack value is introduced. A path generation algorithm based on attack value, BuildNAP, is proposed to eliminate redundant paths. Finally, the PANAG model is used to quantitatively analyze the possibility of different intrusion paths based on intrusion intent, and predict the attack path that the attacker is most likely to take. Experimental results demonstrate the accuracy and execution efficiency of the proposed method.

[Key words] state transition; Node Vulnerability Clustering(NVC); attack value; attack feasibility; intrusion intent

DOI: 10.19678/j.issn.1000-3428.0055651

0 概述

随着互联网的快速发展, 网络空间安全问题日益突出。2018 年, CNCERT 全年截获计算机恶意程序超过 1 亿个, 其中包含计算机恶意程序家族超过 51 万个, 比 2017 年增加 8 132 个, 全年计算机恶意程序传播次数日均达 500 万余次^[1]。上述数据表明, 网络攻击造成的安全问题已不容忽视, 制定有效的安全防护措施尤为重要。攻击路径预测是当前主

要的主动防御技术之一, 其通过分析网络中弱点关联关系来发现攻击者可能采取的攻击路径, 从而为网络防御提供理论依据^[2-3]。目前, 多数学者描述攻击路径时常使用的模型为攻击树和攻击图。攻击树具有直观、可视化的层次结构, 对攻击行为具有较好的图形化描述效果, 但其存在扩展性较弱的问题, 不适用于大规模复杂网络^[4]。攻击图具有良好的扩展性, 能够清晰地表达节点之间的依赖关系, 为描绘攻击路径提供了一种可视化方法^[5]。此外, 网络攻击

基金项目: 国家自然科学基金(61300216)。

作者简介: 王 辉(1975—), 男, 教授、博士, 主研方向为网络安全; 赵 雅、张 娟, 硕士研究生; 刘 琨(通信作者), 副教授。

收稿日期: 2019-08-05 修回日期: 2019-10-04 E-mail: 763471003@qq.com

通常带有主观因素,具有不确定性,攻击图能够描述攻击者可能采取的所有攻击行为,其具有处理不确定性关系的能力^[6-7]。因此,利用攻击图预测攻击者可能采取的攻击路径成为近年来学者们广泛关注的一个研究热点。

文献[8]提出基于 D-S 证据理论的攻击路径预测方法,其应用概率推理计算攻击路径发生的可能性。文献[9]通过分析攻击行为发生的不确定性,提出一种综合预测算法。文献[10]通过概率攻击图推理攻击节点的可达性,根据节点状态及节点间的关联关系预测可能发生的攻击行为。文献[11]分析网络安全态势要素,构建威胁状态转移图用于实时预测网络安全态势,从而提高攻击路径预测的效果。上述方法主要依据当前网络状态对未来可能的攻击行为进行预测,具有一定的可行性,然而却忽略了攻击者将目标节点的成本和收益作为攻击依据的现象,从而导致路径冗余问题,影响了攻击路径概率的准确计算。

文献[12]针对攻击发生的不确定性问题,将概率属性添加到攻击图模型中,利用攻击图来推测关键攻击路径,但随着网络规模的不断扩大,其生成的攻击图可能存在状态爆炸问题。文献[13]利用贝叶斯网络将节点置信度转化为对攻击节点成本和收益的计算,对比不同节点的成本-收益来找出最可能的攻击路径,但其未对节点中的弱点进行属性分析,导致预测准确度较低。文献[14]构建模糊马尔科夫链模型对网络攻击路径进行预测,该模型的关键是确定适合的隶属函数,当前常用的隶属函数选取方法有模糊统计法、判别矩阵法以及例证法等,但上述方法都带有主观性,理论基础较弱,存在预测通用性较低的问题。文献[15]设计因果知识网络描述网络入侵过程,并给出改进的 Dijkstra 算法来识别入侵意图和预测不同水平的攻击者在攻击路径选择上的差异性。该方法预测准确率较高但计算较为复杂,存在预测成本较高的问题。文献[16]通过综合分析攻击者、防御者以及网络环境三方面要素的相互关系,设计基于动态贝叶斯攻击图的攻击路径预测算法,但其网络攻防具有动态性的特点,文中节点概率计算方式并不能实时描绘攻防双方的对抗特征,导致预测效果不佳。

为避免攻击图生成的状态爆炸问题,本文提出节点弱点聚类算法 NVC 和概率属性网络攻击图生成算法 GeneratNAG。通过分析影响网络攻击行为的多方面因素,设计基于攻击价值的攻击路径生成算法 BuildNAP。利用优化后的攻击路径,应用概率推理思想计算基于入侵意图的不同攻击路径的发生概率,以预测攻击者最可能采取的攻击路径。

1 PANAG 定义及 NAP 描述

攻击路径预测是以图的形式寻找攻击者为实现

入侵意图而可能采取的所有攻击路径。本文通过对网络中的弱点属性进行分析,构建概率属性网络攻击图模型,管理员能够依据此模型分析出最大概率攻击路径,从而进行防御决策。给出概率属性网络攻击图、攻击路径定义如下:

定义 1 (概率属性网络攻击图) 设 $PANAG = (V, H, E, P, P', T, W)$ 为有向无环图,其中:

1) $V = \{ \forall v_i \in V, v_i \text{ 为一个弱点} \}$ 为网络中的弱点集合。若攻击者能够成功利用主机中的弱点,则会给网络带来安全隐患。

2) $H = \{ H_i | i = 1, 2, \dots, N \}$ 为攻击图中包含弱点的主机节点集合。其中, $H_i = \{ v_j, v_{j+1}, \dots, v_m \} (0 < j < m)$ 为攻击图中的某一个节点,共含有 $m - j + 1$ 个弱点, N 为节点的个数。

3) $E = \{ e_{k \rightarrow r} | k = 1, 2, \dots, N, r = 1, 2, \dots, N \}$ 为攻击图中节点之间存在关联关系的有向边集合,也即攻击行为集合。有向边 $\langle H_k, H_r \rangle$ 的攻击行为可表示为 $e_{k \rightarrow r}$ 。

4) P 代表弱点被成功利用的概率,即节点可达概率,其由弱点的属性决定,具体计算详见 2.1 节。

5) P' 代表攻击者采取一系列相关攻击行为后,实现入侵意图的攻击路径相对概率。假设攻击图中包含 L 条实现入侵意图的攻击路径,用 Θ 表示攻击者的入侵意图,则每条攻击路径的相对概率则表示为 $P'(NAP_l | \Theta)$, 其中, NAP_l 为攻击路径, $l = 1, 2, \dots, L$ 。

6) $T = \{ t_{n \rightarrow p} | n = 1, 2, \dots, N, p = 1, 2, \dots, N \}$ 代表攻击图包含的节点状态变迁集合, $t_{n \rightarrow p}$ 表示攻击者在占有当前节点 H_n 的情况下成功占有下一个目标节点 H_p 并完成攻击行为 $e_{n \rightarrow p}$ 的节点变迁。

7) W 代表攻击价值集合, $\forall w \in W$ 依附于攻击图的有向边,其由攻击成本与攻击收益共同决定,计算公式详见 3.3 节。

定义 1 主要综合上述 7 种因素及相互关系给出概率属性网络攻击图模型。依照定义 1,借助弱点扫描工具对目标网络中的设备进行扫描,将具有弱点的主机作为攻击图节点,有向边代表节点之间的关联关系,生成如图 1 所示的简单攻击图。

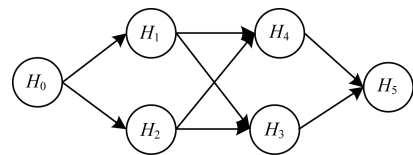


图 1 简单攻击图

Fig. 1 Simple attack graph

在图 1 中,攻击者从初始节点 H_0 出发到成功占有 H_5 最终实现入侵意图,共包含 8 次不同的攻击行为,分别为 $e_{0 \rightarrow 1}, e_{0 \rightarrow 2}, e_{1 \rightarrow 3}, e_{1 \rightarrow 4}, e_{2 \rightarrow 3}, e_{2 \rightarrow 4}, e_{3 \rightarrow 5}, e_{4 \rightarrow 5}$, 相应完成了 8 次状态变迁,分别为 $t_{0 \rightarrow 1}, t_{0 \rightarrow 2}, t_{1 \rightarrow 3}, t_{1 \rightarrow 4}, t_{2 \rightarrow 3}, t_{2 \rightarrow 4}, t_{3 \rightarrow 5}, t_{4 \rightarrow 5}$ 。攻击者从当前所在节点到成功占据下一个关联节点,必定利用了其含有的某

一弱点,因此,依据弱点的属性能够衡量节点的可达性,便于预测攻击者的可能攻击路径。

定义 2 (网络攻击路径(Network Attack Path,NAP)) 对于入侵目标节点 $\forall H_N \in H$,攻击者首先选择初始节点 $\forall H_i \in H$ 发起攻击,其安全状态发生改变后,对其他具有依赖关系的节点 $\forall H_m \in H$ 进行攻击。以此类推,直至最终占有 H_N ,所经过的攻击节点为 H_i, H_m, \dots, H_N ,其中,任意 2 个相邻的节点 $\langle H_i, H_m \rangle$ 满足 $t_{i \rightarrow m} \in T, 0 < i < m \leq N$,且所经过的变迁序列有限,则 $\langle H_i, H_m, \dots, H_N \rangle$ 称为一条攻击路径,记为 NAP。

从定义 2 可以看出,网络攻击路径描述了攻击者实现入侵意图而采取的一系列攻击行为,体现了攻击者对网络中节点作不同选择的可能性。以图 1 为例,共包含如下 4 条攻击路径:

$$NAP_1 = \langle H_0, H_1, H_3, H_5 \rangle$$

$$NAP_2 = \langle H_0, H_1, H_4, H_5 \rangle$$

$$NAP_3 = \langle H_0, H_2, H_3, H_5 \rangle$$

$$NAP_4 = \langle H_0, H_2, H_4, H_5 \rangle$$

图 1 中的攻击者依次占有所有节点后到达 H_5 ,为准确直观地描述概率属性网络攻击图与攻击路径的关联性,对该攻击过程进行如下分析:

1) 在通常情况下,目标节点若含多个攻击效果相同的弱点,则攻击者会选择容易利用的弱点,因此,弱点属性影响节点的可达概率 P 。

2) 在理论上,只需考虑节点的可达概率 P ,由于 $P > 0$,因此攻击者可以从上述 4 条路径中随意挑选路径发起攻击,直至占有 H_5 实现入侵意图。但在实际中,若目标节点的攻击成本高于收益,则攻击者会放弃该节点,即攻击价值在一定程度上决定了攻击行为是否发生。假定 $w(e_{1 \rightarrow 4}) < 0$,攻击者会放弃节点 H_4 的攻击,因此, NAP_2 为无效攻击路径。

3) 若未有效分析攻击图中包含的弱点及攻击路径信息,会导致实现入侵意图的有效攻击路径相对概率 P' 计算有偏差,即存在预测结果不准确的现象。

2 弱点概率属性分析及 PANAG 生成算法

攻击图能够方便管理员对网络整体安全状况进行分析决策,若攻击图过于复杂,则不利于管理员制定合理的防御策略。鉴于此,本文通过对弱点概率属性进行分析,提出节点弱点聚类算法 NVC 和概率属性网络攻击图生成算法 GeneratNAG,从而优化攻击图生成效果,增强其可读性。

2.1 弱点概率属性分析

在实际攻击场景中,能够被攻击者利用的弱点通常含有某种漏洞。攻击者能否实现节点状态变迁与节点是否含有漏洞以及该节点的属性有关。目前,被公认的能够量化漏洞属性的评分工具为通用漏洞评估系统(Common Vulnerability Scoring System, CVSS)^[17],漏洞属性在攻击路径(Access Vector, AV)、

攻击复杂度(Access Complexity, AC)以及身份认证(Authentication, AU)三方面对应等级的具体取值如表 1 所示。

表 1 漏洞属性度量表

CVSS 指标	等级	取值
AV	本地/临近网络/网络	0.395/0.646/1.000
AC	高/中/低	0.35/0.61/0.71
AU	多次/单次/无需认证	0.450/0.560/0.704

因为攻击成功概率与所利用的漏洞属性密切相关,所以本文使用 CVSS 对不同漏洞的属性进行度量,判断漏洞利用的难易程度,并以此为依据计算攻击者的攻击成功概率,即节点可达概率 P ,其计算公式如下:

$$P = AC \times AV \times AU \quad (1)$$

2.2 PANAG 生成算法

在对网络攻击进行建模时,需要综合分析网络中的拓扑关系和弱点信息。当节点具有很多可以选择利用的弱点时,就会存在多条攻击路径,因此,生成的攻击图会过于复杂。针对该现象,本文提出节点弱点聚类算法 NVC 来简化节点中含有的弱点,然后利用概率属性网络攻击图生成算法 GeneratNAG 生成攻击图。

2.2.1 节点弱点聚类算法 NVC

当攻击者面临目标节点内存在多个弱点可供选择且攻击效果相同时,往往会选择最容易成功利用的弱点。为此,本文先综合分析多种弱点被利用后产生的后果,将攻击分为获取信息(GI)、权限升级(PU)以及拒绝服务(DoS)3 种类型,再采用节点弱点聚类算法 NVC 对节点弱点进行预处理。节点弱点聚类算法流程如图 2 所示。

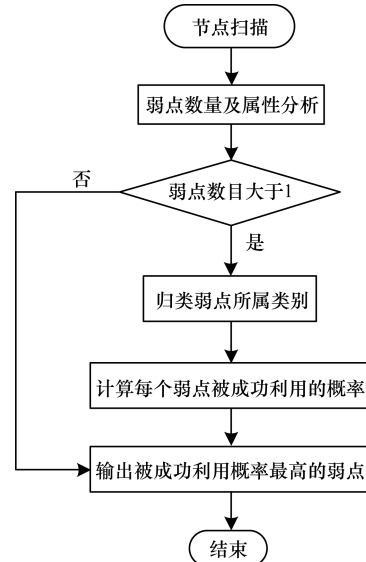


图 2 节点弱点聚类算法流程

Fig. 2 Procedure of node vulnerability clustering algorithm

在节点弱点聚类算法 NVC 中,首先利用扫描工具扫描网络中节点含有的弱点信息并进行属性分析;其次利用 CVSS 中对弱点的度量策略来计算攻击图中节点内每个弱点被攻击成功的概率,对属性相同的弱点进行聚类;最后对同种属性的弱点,利用 CVSS 对弱点的度量策略选择攻击成功概率最高的弱点并作为聚类弱点的代表。NVC 算法能够起到减少弱点数目的作用。

2.2.2 概率属性网络攻击图生成算法 GeneratNAG

随着网络规模的扩大,已有的攻击图生成方法已不能准确描述网络安全状况,为此,本文提出一种新的攻击图生成算法。根据单调性假设,攻击者不会重复和放弃已攻击占有的节点,因此,攻击者必先成功占有前置状态节点,后置状态节点才可能出现,即前置状态节点和后置状态节点互为因果关系。因此,本文采用正向搜索的思想,首先搜索可能存在的攻击实例,接着分析攻击实例内节点间的相互关系,寻找并不断创建网络中新的攻击节点,循环上述操作,直至无新的攻击实例出现,最终生成概率属性网络攻击图。概率属性网络攻击图生成算法 GeneratNAG 具体描述如下:

算法 1 GeneratNAG 算法

输入 初始化攻击节点 s_0 , 攻击实例集合 S

输出 PANAG

1. while $S \neq \emptyset$
2. $S_{Node} \leftarrow S_{Node} \cup \{s_0\}$
3. for each $s \in S$
4. if $H_j \in \text{pre}(s) \subset S_{Node}$ then
5. createNode(H_j) // 创建攻击节点 H_j
6. $A \leftarrow A \cup \{H_j\}$ // A 为攻击图的节点集合
7. for each $H_i \in \text{pre}(s)$
8. $E \leftarrow E \cup \{\langle H_i, H_j \rangle\}$ // E 为攻击图中的边集合
9. for each $H_m \in \text{post}(s)$
10. if $H_m \notin S_{Node}$ then
11. createNode(H_m)
12. $A \leftarrow A \cup \{H_m\}$
13. $E \leftarrow E \cup \{\langle H_j, H_m \rangle\}$
14. $S_{Node} \leftarrow S_{Node} \cup \{H_m\}$ // 更新当前攻击节点
15. $S \leftarrow S - \{s\}$ // 将攻击实例 s 从集合 S 中移除
16. GeneratNAG(PANAG, S)

在算法 1 中,首先收集归纳网络攻击状态前置节点 $\text{pre}(s)$ 和网络攻击状态后置节点 $\text{post}(s)$,即模式化所有可能攻击实例并存储在集合 S 中,作为 GeneratNAG 的输入。算法第 1 行~第 4 行将初始攻击节点 s_0 存储在当前攻击节点集合 S_{Node} 中,并搜索 S 中的节点,判断是否有以当前攻击节点为 $\text{pre}(s)$ 的攻击实例;第 5 行~第 15 行进行判断,若有攻击实例满足上述条件,则创建攻击节点 H_j ,并建立该节点与其前置网络状态节点 H_i 的一条边 $\langle H_i, H_j \rangle$,若该节点的网络状态后置节点 H_m 不属于 S_{Node} ,则建立 H_m 与其 $\text{post}(s)$ 的一条边 $\langle H_j, H_m \rangle$,并将 H_m 加入 S_{Node} 中,

同时将该攻击实例从 S 中移除;第 16 行对于集合 S_{Node} 中新的当前攻击节点,循环执行第 4 行~第 15 行操作,直到 S 为空集。算法第 10 行加入对网络状态后置节点 H_m 与 S_{Node} 的判断,以避免攻击图生成环路。

3 攻击可行性及 NAP 算法分析

随着网络规模的不断上升,相应的主机节点数也会增多,攻击图会包含过多的攻击路径,影响攻击路径的有效预测。针对该问题,本文通过对攻击图中节点的单元攻击成本(Unit Attack Cost, UAC)和单元攻击收益(Unit Attack Revenue, UAR)进行分析,引入攻击价值的概念,提出一种基于攻击价值的攻击路径生成算法。

3.1 单元攻击成本分析

UAC 指攻击者发动一次攻击所消耗的成本,其由操作成本和风险成本组成。本文借鉴文献[18]的思想,定义单元攻击 $e_{i \rightarrow j}$ 的操作成本由元操作成本 $\text{cost}(\text{meta-operations})$ 和操作序列成本 $\text{cost}(\text{sequence})$ 构成,计算公式如下:

$$\text{cost}(e_{i \rightarrow j})_{\text{operation}} = \alpha \times \text{cost}(\text{meta-operations}) + \beta \times \text{cost}(\text{sequence}) \quad (2)$$

其中, α, β 为元操作成本和操作序列成本所对应的权重。

关于单元攻击操作成本的详细描述可参见文献[18]。攻击行为的风险成本应根据具体的攻击场景进行量化,通常由风险系数和攻击者累积的攻击经验决定。攻击者每发动一次攻击都会存在被发现的可能,为此定义风险系数(δ)描述单元攻击被发现的可能性大小。若攻击者认为目标节点对于实现入侵意图具有重要性,则该节点就很容易被攻击,也很容易检测到该攻击行为。因此,定义节点重要度(M)作为风险成本评估因素。此外,风险成本与攻击者的攻击行为复杂度(φ)也具有相关性,攻击行为复杂度越高,越容易利用节点中的弱点,但面临的风险也越大。因此,风险系数 δ 的数学模型如下:

$$\delta(e_{i \rightarrow j}) = M(e_{i \rightarrow j}) \times \varphi(e_{i \rightarrow j}) \quad (3)$$

由于攻击者是理智的,当攻击者采取的攻击次数越多时,经验就越丰富,其被发现的风险成本就越小。因此,定义风险成本的数学模型如下:

$$\text{cost}(e_{i \rightarrow j})_{\text{risk}} = \eta(e_{i \rightarrow j})^{n-1} \times \delta(e_{i \rightarrow j}) \quad (4)$$

其中, $\eta(e_{i \rightarrow j})$ 为攻击者经验依赖系数, n 为成功攻击的次数。式(3)、式(4)中的相关变量具体取值均结合实际网络攻击场景并由专家经验给出。经过分析,本文建立单元攻击成本的计算模型如下:

$$\text{UAC}(e_{i \rightarrow j}) = \rho \times \text{cost}(e_{i \rightarrow j})_{\text{operation}} + \nu \times \text{cost}(e_{i \rightarrow j})_{\text{risk}} \quad (5)$$

其中, ρ, ν 分别代表操作成本和风险成本的权重,且满足 $\rho + \nu = 1$ 。

3.2 单元攻击收益分析

UAR 是指攻击者采取单元攻击后获得的收益。

通常很难具体量化收益,本文用节点的资源损失(Resource Loss, RL)来表示 UAR。

定义 3(资源损失) 资源损失代表节点受到某类攻击行为所遭受的损失大小。本文参考文献[19],用攻击致命度(Attack Fatality, AF)、危险度(Risk)以及安全属性 3 个因素描述攻击的节点资源损失。

定义 4(攻击致命度) 攻击致命度代表节点受到某类攻击行为所产生的危害水平,可以用 0~N 之间的数值来表示各类攻击的相对危害大小。依据 2.2.1 节对攻击的分类,相同类型的攻击行为赋予相同的致命度等级,具体取值如表 2 所示。

表 2 攻击致命度等级表
Table 2 Attack fatality rating table

分类	等级 (AF)
权限升级	5
获取信息	3
拒绝服务	1

目前被广大研究人员认可的能反映节点资源的安全特性为完整性、保密性和可用性,因此,本文采用三元组(L_i, L_c, L_a)分别表示单元攻击行为对节点资源三方面安全特性的不同致命度偏重,取值范围均为[0,1]。

定义 5(危险度) 危险度表示攻击者的目标攻击节点所面临的危险程度。节点的危险度可采用 high、middle 和 low 3 个等级来描述。攻击者成功利用危险度越高的节点,相应的资源损失就越大,危险度等级具体取值由实际攻击场景确定。

本文结合网络具体环境,定义 $Base_v$ 为节点资源价值基数,用 Risk 和 $Base_v$ 表示网络中各个节点的相对价值 Value,即 $Value = Risk \times Base_v$ 。此外,节点的资源价值相对于安全属性往往具有一定偏重,用(P_i, P_c, P_a)描述对属性的完整性、机密性和可用性的不同偏重,且满足 $P_i + P_c + P_a = 1$ 。经上述分析,给出单元攻击 $e_{i \rightarrow j}$ 攻击成功后对网络中节点造成的资源损失计算模型如下:

$$RL(e_{i \rightarrow j}) = AF \times Value \times (L_i \times P_i + L_c \times P_c + L_a \times P_a) \quad (6)$$

可以认为单元攻击 $e_{i \rightarrow j}$ 对节点造成的资源损失就是本次攻击的收益,即:

$$UAR(e_{i \rightarrow j}) = RL(e_{i \rightarrow j}) \quad (7)$$

3.3 攻击可行性分析

在通常情况下,攻击者对网络中的目标节点实施攻击时,会对该节点的攻击价值 w 进行综合考量,当攻击者认为本次攻击的攻击价值在目标范围内时才会采取攻击行为。因此,本文给出式(8)计算攻击价值 w ,从而判断攻击行为的可行性:

$$w = UAR(e_{i \rightarrow j}) - UAC(e_{i \rightarrow j}) \quad (8)$$

从式(8)可以看出,攻击可行性由节点的单元攻击成本和单元攻击收益共同决定。从攻击者的角度

考虑,若攻击者认为节点的单元攻击成本高于收益(此时 $w < 0$),就会放弃对该节点的攻击而寻找其他可行目标节点。对攻击价值的分析在一定程度上能够消除攻击路径冗余,提高攻击预测的准确度。

3.4 攻击路径生成算法描述

定义 6(偏序关系集(Partially Ordered Set, POS)) PANAG 中的 2 个任意相邻节点 H_i 和 H_m ,如果 H_i, H_m 之间存在一条 $\langle H_i, H_m \rangle$ 有向边,则称 $\langle H_i, H_m \rangle$ 具有偏序关系。所有偏序关系构成的集合称为偏序关系集,记作 POS。

为详细展示 NAP 的形成过程,用 true 代表状态变迁和攻击行为发生,false 代表不可能发生。通过对某目标网络中的节点进行弱点分析,得到其含有的攻击图,依据上文的攻击可行性分析并结合专家经验为攻击图赋予攻击价值 w ,然后以 H_0 为起始点,断开以其为节点的一条边,存放入 POS_i 中,之后依照某一拓扑顺序 $e_{i \rightarrow j}$ 逐渐得到 POS。赋予 w 后的攻击图如图 3 所示。

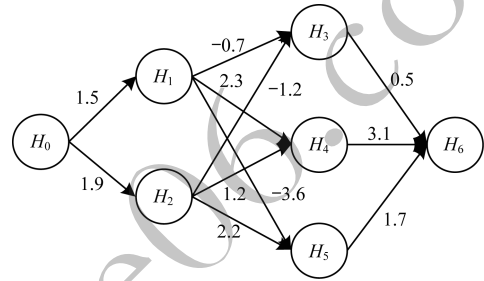


图 3 赋予攻击价值的攻击图

Fig. 3 Attack graph with attack value

在图 3 中,拓扑序 $\phi = \{e_{0 \rightarrow 1}, e_{0 \rightarrow 2}, e_{1 \rightarrow 3}, e_{1 \rightarrow 4}, e_{2 \rightarrow 4}, e_{2 \rightarrow 5}, e_{2 \rightarrow 6}, e_{3 \rightarrow 6}, e_{4 \rightarrow 6}, e_{5 \rightarrow 6}\}$,具体流程如下:

- 1) 断开 $e_{0 \rightarrow 1}$, $w = 1.5 > 0$, $e_{0 \rightarrow 1} \leftarrow \text{true}$, $t_{0 \rightarrow 1} \leftarrow \text{true}$, $POS_0 = \{\langle H_0, H_1 \rangle\}$ 。
- 2) 断开 $e_{0 \rightarrow 2}$, $w = 1.9 > 0$, $e_{0 \rightarrow 2} \leftarrow \text{true}$, $t_{0 \rightarrow 2} \leftarrow \text{true}$, $POS_1 = POS_0 \cup \{\langle H_0, H_2 \rangle\}$ 。
- 3) 断开 $e_{1 \rightarrow 3}$, $w = -0.7 < 0$, $e_{1 \rightarrow 3} \leftarrow \text{false}$, $t_{1 \rightarrow 3} \leftarrow \text{false}$ 。
- 4) 断开 $e_{1 \rightarrow 4}$, $w = 2.3 > 0$, $e_{1 \rightarrow 4} \leftarrow \text{true}$, $t_{1 \rightarrow 4} \leftarrow \text{true}$, $POS_2 = POS_1 \cup \{\langle H_1, H_4 \rangle\}$ 。
- 5) 断开 $e_{1 \rightarrow 5}$, $w = -3.6 < 0$, $e_{1 \rightarrow 5} \leftarrow \text{false}$, $t_{1 \rightarrow 5} \leftarrow \text{false}$ 。
- 6) 断开 $e_{2 \rightarrow 3}$, $w = -1.2 < 0$, $e_{2 \rightarrow 3} \leftarrow \text{false}$, $t_{2 \rightarrow 3} \leftarrow \text{false}$ 。
- 7) 断开 $e_{2 \rightarrow 4}$, $w = 1.2 > 0$, $e_{2 \rightarrow 4} \leftarrow \text{true}$, $t_{2 \rightarrow 4} \leftarrow \text{true}$, $POS_3 = POS_2 \cup \{\langle H_2, H_4 \rangle\}$ 。
- 8) 断开 $e_{2 \rightarrow 5}$, $w = 2.2 > 0$, $e_{2 \rightarrow 5} \leftarrow \text{true}$, $t_{2 \rightarrow 5} \leftarrow \text{true}$, $POS_4 = POS_3 \cup \{\langle H_2, H_5 \rangle\}$ 。
- 9) 断开 $e_{3 \rightarrow 6}$, $w = 0.5 > 0$, $e_{3 \rightarrow 6} \leftarrow \text{true}$, $t_{3 \rightarrow 6} \leftarrow \text{true}$, $POS_5 = POS_4 \cup \{\langle H_3, H_6 \rangle\}$ 。
- 10) 断开 $e_{4 \rightarrow 6}$, $w = 3.1 > 0$, $e_{4 \rightarrow 6} \leftarrow \text{true}$, $t_{4 \rightarrow 6} \leftarrow \text{true}$, $POS_6 = POS_5 \cup \{\langle H_4, H_6 \rangle\}$ 。

11) 断开 $e_{5 \rightarrow 6}$, $w = 1.7 > 0$, $e_{5 \rightarrow 6} \leftarrow \text{true}$, $t_{5 \rightarrow 6} \leftarrow \text{true}$, $\text{POS}_7 = \text{POS}_6 \cup \{ \langle H_5, H_6 \rangle \}$ 。

12) 遍历变迁关系集合 T , 查找标识为 false 的 $t_{i \rightarrow j}$ 并将其从 T 中移除。

13) 若 $T \neq \emptyset$, 依据 POS 得到攻击路径 NAP_i :

$\text{NAP}_1 = \langle H_0, H_1, H_4, H_6 \rangle$

$\text{NAP}_2 = \langle H_0, H_2, H_4, H_6 \rangle$

$\text{NAP}_3 = \langle H_0, H_2, H_5, H_6 \rangle$

由上述结果可以看出,该方法通过对攻击价值 w 的判断,对攻击行为和状态变迁进行标识,舍弃标识为 false 的状态变迁,有效减少了冗余路径。基于攻击价值的攻击路径生成算法 BuildNAP 具体描述如下:

算法2 BuildNAP 算法

输入 PANAG, 偏序关系集 POS, 攻击价值 w , 变迁关系集 T , 有向边集合 E , 拓扑序 φ , 任意节点 H_i, H_j

输出 攻击路径集合 NAP

1. $\varphi \leftarrow \text{PANAG}$, $\text{POS}_i \leftarrow \emptyset$, $T_i \leftarrow \emptyset$

2. FOR (根据 φ 查找每一个节点变量 H_i)

3. 在 PANAG 中找出与 H_i 存在变迁关系的节点 H_j

4. IF ($e_{i \rightarrow j} \in E$)

5. IF ($w > 0$)

6. $e_{i \rightarrow j} \leftarrow \text{true}$, $t_{i \rightarrow j} \leftarrow \text{true}$

7. ELSE

8. $e_{i \rightarrow j} \leftarrow \text{false}$, $t_{i \rightarrow j} \leftarrow \text{false}$

9. END IF

10. $\text{POS}_i \cup \{ \langle H_i, H_j \rangle \}$

11. END IF

12. END FOR

13. 遍历集合 T , 移除所有标识为 false 的 $t_{i \rightarrow j}$

14. IF ($T \neq \emptyset$)

15. $\text{NAP}_i \leftarrow \text{POS}$

16. RETURN NAP_i

4 基于 PANAG 模型的入侵预测

攻击者能否实现入侵意图通常与网络中节点之间的依赖关系以及节点包含的弱点属性有关。然而,由于网络规模的不断扩大,攻击者可以通过多条路径实现其入侵意图。因此,预先发现攻击者的入侵意图并及时掌握其可能实施的攻击路径,有助于防御网络入侵。

4.1 入侵意图的可达性分析

给定 PANAG 模型,如果存在任意节点 $H_i, H_j \in \text{PANAG}$, H_i 为攻击者初始所在节点, H_j 为攻击者完成入侵意图 Θ 的前置条件节点,若模型中含有以 H_i 为起始节点、 H_j 为最终节点的攻击路径 $\langle H_i, H_{i+1}, \dots, H_j \rangle$, 则称入侵意图 Θ 可达。

4.2 入侵意图的实现概率分析

在概率属性网络攻击图中,若攻击者想要占有的目标节点 h 含有多个弱点,利用节点弱点聚类算法 NVC 能够找出攻击者最可能占有的弱点,根据该弱点属性计算节点 h 的可达概率为 $P(h)$ 。假设有

L 条 NAP 能够实现入侵意图,每条 NAP 的对应节点数为 ϕ (不同的 NAP 其 ϕ 取值可能不同),则入侵意图 Θ 的实现概率计算公式为:

$$P(\Theta) = 1 - \prod_L \left[1 - \prod_{\phi} P(h_{\phi}) \right] \quad (9)$$

根据贝叶斯公式可计算出每条 NAP 的入侵意图 Θ 的相对实现概率,如下:

$$P'(\text{NAP}_l | \Theta) = P(\text{NAP}_l) P(\Theta | \text{NAP}_l) \quad (10)$$

其中, $l = 1, 2, \dots, L$ 。依据式 (10) 可找出实现入侵意图概率最大的攻击路径,即攻击者最可能采取的攻击路径。

5 仿真验证

5.1 仿真网络环境

为验证本文提出的模型和算法的有效性与适用性,搭建一个仿真网络环境进行测试分析,其拓扑结构如图 4 所示。

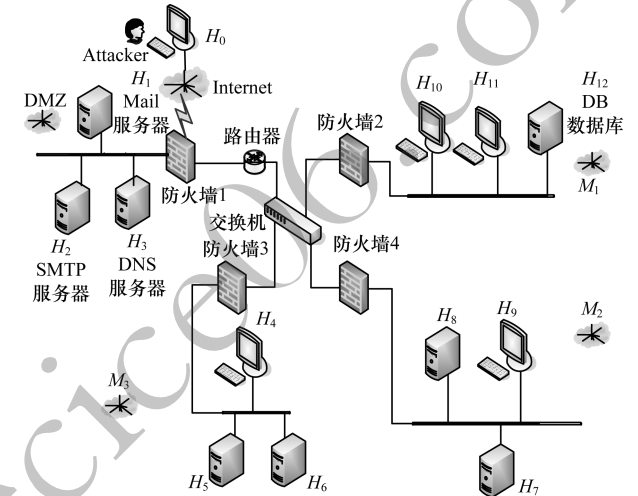


图4 仿真网络拓扑

Fig.4 Simulation network topology

仿真网络包括 M_1 、 M_2 、 M_3 以及 DMZ 4 个安全区域,每个安全区域内节点之间可任意访问。DMZ 中包含 Mail 服务器、SMTP 服务器以及 DNS 服务器,防火墙 3 保护 DMZ 区连接 Internet。区域 M_2 和 M_3 内的主机均可与 DMZ 中的 3 台服务器互相访问,区域 M_1 与 DMZ 不能互相访问。区域 M_3 中的主机 H_4 能够访问区域 M_2 中的服务器 H_{12} ,同时 H_4 和 M_2 中的主机 H_9 与区域 M_1 中的 DB 服务器能够互相访问。攻击者通过 Internet 访问该网络。

在网络节点上配置的相关弱点信息如表 3 所示。假定攻击者的入侵意图是窃取区域 M_1 中 DB 服务器 H_{12} 的隐秘数据和敏感信息,为简化攻击行为的可行性分析,本文首先依据文中的单元攻击成本、单元攻击收益的数学模型并结合专家经验,将节点 H_2 的攻击价值 w 赋值为 -1.2 ,图 4 中其他节点的攻击价值 w 均大于 0。

表 3 节点弱点信息

Table 3 Node vulnerability information

节点	编号	弱点信息	类型
H_1	v_1	CVE-2011-1283	PU
H_1	v_2	CVE-2015-2453	PU
H_2	v_3	CVE-2004-2527	DoS
H_2	v_4	CVE-2013-2968	DoS
H_2	v_5	CVE-2013-2783	DoS
H_3	v_6	CVE-2004-1453	GI
H_4	v_7	CVE-2016-3055	DoS
H_4	v_8	CVE-2015-4936	DoS
H_8	v_9	CVE-2015-2471	GI
H_8	v_{10}	CVE-2013-3686	GI
H_8	v_{11}	CVE-2004-1453	GI
H_8	v_{12}	CVE-2006-5913	GI
H_9	v_{13}	CVE-2004-0812	PU
H_9	v_{14}	CVE-2015-2453	PU
H_9	v_{15}	CVE-2012-5613	PU
H_{12}	v_{16}	CVE-2000-0148	GI

5.2 仿真结果及分析

首先利用节点弱点聚类算法 NVC 对该网络中的弱点进行预处理,输出每个节点聚类后的弱点,并依据式(1)计算出所有包含弱点的节点可达概率 P ,如表 4 所示。

表 4 节点弱点聚类信息

Table 4 Node vulnerability clustering information

节点	弱点信息	节点可达概率 P	类型
H_1	CVE-2015-2453	0.25	PU
H_2	CVE-2013-2783	0.43	DoS
H_3	CVE-2004-1453	0.20	GI
H_4	CVE-2015-4936	0.50	DoS
H_8	CVE-2006-5913	0.50	GI
H_9	CVE-2012-5613	0.34	PU
H_{12}	CVE-2000-0148	0.50	GI

根据网络的节点弱点和拓扑结构信息,利用本文给出的概率属性网络攻击图生成算法 GenerateNAG 生成该网络的攻击图,如图 5 所示。

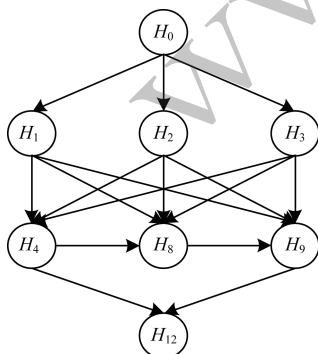


图 5 概率属性网络攻击图

Fig. 5 Probability attribute network attack graph

针对得出的 PANAG 模型,根据本文提出的攻击可行性分析方法,利用攻击路径生成算法 BuildNAP 生成 8 条可行的攻击路径,如表 5 所示。在表 5 中,CP 代表攻击路径的可达概率,其为每条攻击路径所经过的各节点可达概率之积。

表 5 实现入侵意图的路径信息

Table 5 Path information to achieve intrusion intent

编号	攻击路径	CP	P'
NAP ₁	$\langle H_0, H_1, H_4, H_{12} \rangle$	0.063	0.116
NAP ₂	$\langle H_0, H_1, H_8, H_9, H_{12} \rangle$	0.009	0.017
NAP ₃	$\langle H_0, H_1, H_9, H_{12} \rangle$	0.042	0.077
NAP ₄	$\langle H_0, H_1, H_4, H_8, H_9, H_{12} \rangle$	0.011	0.020
NAP ₅	$\langle H_0, H_3, H_4, H_{12} \rangle$	0.050	0.092
NAP ₆	$\langle H_0, H_3, H_8, H_9, H_{12} \rangle$	0.017	0.031
NAP ₇	$\langle H_0, H_3, H_9, H_{12} \rangle$	0.030	0.055
NAP ₈	$\langle H_0, H_3, H_4, H_8, H_9, H_{12} \rangle$	0.008	0.015

利用式(9)计算攻击者的入侵意图 Θ 的实现概率为 $P(\Theta) = 0.423$,通过式(10)计算得出攻击者实现入侵意图的每条攻击路径的相对概率 P' ,具体结果为表 5 中第 4 列所示。由此可以看出, $P'(\text{NAP}_1 | \Theta)$ 的取值最大,因此, NAP_1 为最可能采取的攻击路径,管理员应对此进行重点防御。

5.3 仿真结果比较

本文利用节点弱点聚类算法以有效简化网络中的弱点,并给出攻击可行性的判断依据,消除了冗余攻击路径。经过对已有研究的对比分析得出,文献[9,20]与本文研究方法有一定的相似性。为此,本文进行 3 组仿真实验,在攻击图生成效果、执行时间以及预测有效性 3 个方面进行综合对比,结果如下:

1) 攻击图生成效果对比。为保证仿真结果的可比性,进行与本文算法相同的仿真环境配置,使用文献[20]攻击图生成算法生成攻击图,结果如图 6 所示。

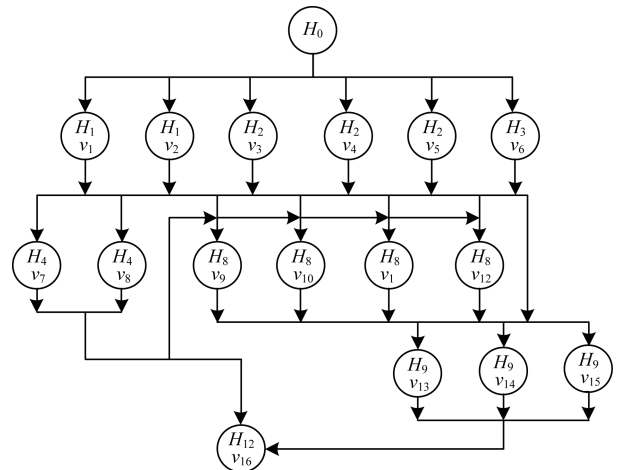


图 6 文献[20]算法攻击图生成效果

Fig. 6 Attack graph generation effect of the algorithm in reference [20]

从图6可以看出,文献[20]算法生成的攻击图中攻击者利用节点的不同弱点实现入侵意图,但存在过多的冗余路径,可读性差。本文算法从攻击者角度考虑,对生成的概率属性网络攻击图和攻击路径进行有效简化,能够更加清楚地描述节点关系,有助于攻击路径预测。

2) 执行时间对比。将本文算法与文献[20]算法的攻击图生成时间进行对比,首先在网络中随机增加主机节点数、拓扑关系及弱点数,然后分别计算2种算法的执行时间,结果如图7所示。

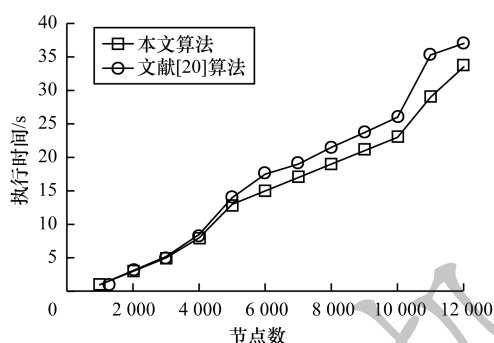


图7 2种算法的攻击图生成时间对比

Fig.7 Comparison of attack graph generation time of two algorithms

从图7可以看出,当主机节点数小于4 000时,2种算法的执行时间均低于10 s,随着节点数的增多,2种算法的执行时间都明显上升;当节点数不超过5 000时,2种算法所需执行时间基本上保持相同;当节点数大于5 000时,本文算法的时间消耗明显少于文献[20]算法,说明本文算法更适用于大规模复杂网络。

3) 预测性能对比。为验证本文算法的有效性,将其与文献[9,20]算法进行对比,预测准确率结果如表6所示。

表6 预测准确率对比

Table 6 Comparison of prediction accuracy %

实验次数	本文算法	文献[9]算法	文献[20]算法
50	94.0	92.0	90.0
100	97.0	93.0	92.0
150	96.5	93.0	91.0
200	95.0	94.5	94.0
300	97.5	94.0	93.5
500	98.5	96.0	95.0

从表6可以看出,相比于文献[9,20]算法,本文算法的准确率更高,主要是因为本文利用节点弱点聚类算法选出了攻击者最可能利用的弱点,并以此为依据计算攻击者的最大概率攻击路径。

6 结束语

面对复杂的网络环境,进行攻击路径预测有助于管理员分析网络安全状况。针对现有攻击图生成方法复杂度高、可读性差的问题,本文提出节点弱点聚类算法NVC和概率属性网络攻击图生成算法GeneratNAG。通过分析影响攻击可行性的因素,设计基于攻击价值的攻击路径生成算法BuildNAP。在此基础上,应用概率推理预测攻击者最可能采取的攻击路径。实验结果验证了本文算法较高的准确性。本文综合分析影响网络攻击行为的多方面因素,给出了节点的攻击价值计算方式,但其中涉及较多参数,且只能依据专家经验给出取值。为提高算法执行效率,下一步将利用数学模型来计算具体的参数数值。

参考文献

- [1] National Internet Emergency Center. Overview of China's Internet security situation in 2018 [EB/OL]. [2019-07-20]. <https://www.cert.org.cn/publish/main/46/index.html>. (in Chinese)
国家互联网应急中心. 2018年我国互联网安全态势综述[EB/OL]. [2019-07-20]. <https://www.cert.org.cn/publish/main/46/index.html>.
- [2] ABRAHAM S, NAIR S. A predictive framework for cyber security analytics using attack graphs [J]. International Journal of Computer Networks and Communications, 2015, 7(1): 1-17.
- [3] BAO Xuhua, DAI Yingxia, FENG Pinghui, et al. Detection and prediction algorithm of compound attack based on intrusion intention [J]. Journal of Software, 2005, 16(12): 2132-2138. (in Chinese)
鲍旭华,戴英侠,冯萍慧,等. 基于入侵意图的复合攻击检测和预测算法[J]. 软件学报, 2005, 16(12): 2132-2138.
- [4] WHITLEY J N, PHAN RAPHAEL C W, WANG J, et al. Attribution of attack trees [J]. Computers and Electrical Engineering, 2011, 37(4): 624-628.
- [5] WANG Hui, WANG Tengfei, LIU Shufen. A network attack path prediction method based on ATI [J]. Computer Engineering, 2016, 42(9): 132-137. (in Chinese)
王辉,王腾飞,刘淑芬. 一种基于ATI的网络攻击路径预测方法[J]. 计算机工程, 2016, 42(9): 132-137.
- [6] YE Ziwei, GUO Yuanbo, WANG Chendong, et al. Survey on application of attack graph technology [J]. Journal on Communications, 2017, 38(11): 121-132. (in Chinese)
叶子维,郭渊博,王宸东,等. 攻击图技术应用研究综述[J]. 通信学报, 2017, 38(11): 121-132.
- [7] LIU Zhenyu, CHEN Yuzhong, GUO Kun, et al. Distributed process mining and graph segmentation for network attack modeling [J]. Journal of Chinese Computer Systems, 2020, 41(8): 1732-1740. (in Chinese)

- 刘贞宇,陈羽中,郭昆,等. 面向网络攻击建模的分布式过程挖掘与图分割方法[J]. 小型微型计算机系统, 2020,41(8):1732-1740.
- [8] QU Zhaoyang, LI Yaying. A network security situation evaluation method based on DS evidence theory [C]// Proceedings of the 2nd Conference on Environmental Science and Information Application Technology. Washington D. C. , USA: IEEE Press, 2010:496-499.
- [9] GHASEMIGOL M, GHAEEMI-BAFGHI A, TAKABI H. A comprehensive approach for network attack forecasting[J]. Computers and Security, 2016, 58:83-105.
- [10] CHEN Xiaojun, SHI Jinqiao, XU Fei, et al. Algorithm of optimal security hardening measures against insider threat[J]. Journal of Computer Research and Development, 2014, 51(7): 1565-1577. (in Chinese)
陈小军, 时金桥, 徐菲, 等. 面向内部威胁的最优安全策略算法研究[J]. 计算机研究与发展, 2014, 51(7): 1565-1577.
- [11] LÜ Huiying, PENG Wu, WANG Ruimei, et al. A real-time network threat recognition and assessment method based on association analysis of time and space[J]. Journal of Computer Research and Development, 2014, 51(5):1039-1049. (in Chinese)
吕慧颖, 彭武, 王瑞梅, 等. 基于时空关联分析的网络实时威胁识别与评估[J]. 计算机研究与发展, 2014, 51(5):1039-1049.
- [12] WANG L Y, ISLAM T, LONG T, et al. An attack graph-based probabilistic security metric [M]//NIKLAS E, NIKLAS S. Lecture notes in computer science. Berlin, Germany: Springer, 2008:283-296.
- [13] DEWRI R, RAY I, POOLSAPPASIT N, et al. Optimal security hardening on attack tree models of networks: a cost-benefit analysis[J]. International Journal of Information Security, 2012, 11(3):167-188.
- [14] KUANG G C, WANG X F, YIN L R. A fuzzy forecast method for network security situation based on Markov [C]// Proceedings of 2012 International Conference on Computer Science and Information Processing. Washington D. C. , USA: IEEE Press, 2012:785-789.
- [15] WANG Shuo, TANG Guangming, KOU Guang, et al. Attack path prediction method based on causal knowledge[J]. Journal on Communications, 2016, 37(10):188-198. (in Chinese)
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.
- [16] HU Hao, YE Runguo, ZHANG Hongqi, et al. Quantitative method for network security situation based on attack prediction[J]. Journal on Communications, 2017, 38(10):122-134. (in Chinese)
胡浩, 叶润国, 张红旗, 等. 基于攻击预测的网络安全态势量化方法[J]. 通信学报, 2017, 38(10):122-134.
- [17] HOLM H, AFRIDI K K. An expert-based investigation of the common vulnerability scoring system [J]. Computers and Security, 2015, 53:18-30.
- [18] WANG Hui, LIU Shufen. A scalable predicting model for insider threat [J]. Chinese Journal of Computers, 2006, 29(8):1346-1355. (in Chinese)
王辉, 刘淑芬. 一种可扩展的内部威胁预测模型[J]. 计算机学报, 2006, 29(8):1346-1355.
- [19] JIANG Wei. Research on key technologies of active defense based on attack defense game model [D]. Harbin: Harbin Institute of Technology, 2010. (in Chinese)
姜伟. 基于攻防博弈模型的主动防御关键技术研究[D]. 哈尔滨: 哈尔滨工业大学, 2010.
- [20] ZHONG Shangqin, XU Guosheng, YAO Wenbin, et al. Network security analysis based on host-security-group[J]. Journal of Beijing University of Posts and Telecommunications, 2012, 35(1):19-23. (in Chinese)
钟尚勤, 徐国胜, 姚文斌, 等. 基于主机安全组划分的网络安全分析[J]. 北京邮电大学学报, 2012, 35(1):19-23.

编辑 吴云芳