基于贝叶斯攻击图的网络安全量化评估研究*

方 研[1], 殷肖川[1], 李景志[2]
(1. 空军工程大学 信息与导航学院 指挥系统技术教研部, 西安 710077; 2. 西安通信学院, 西安 710000)

摘 要: 针对攻击图在评估网络安全时节点关系复杂、存在含圈攻击路径、只能反映网络静态风险等问题,将攻击图与贝叶斯理论结合,提出贝叶斯攻击图的概念,简化了攻击图并通过优化算法避免了含圈路径的产生;通过引入攻击证据与 CVSS 评分系统,提出了一种新的面向脆弱点的网络安全量化评估方法,基于贝叶斯攻击图对网络整体及局部的安全状况进行实时动态评估。通过在实际网络中的实验验证了该方法的可行性及有效性,与传统评估方法相比,该方法能够动态地反映网络安全的态势变化情况。

关键词: 贝叶斯攻击图; 脆弱点; 动态评估; 攻击证据
中图分类号: TP393.08 **文献标志码**: A **文章编号**: 1001-3695(2013)09-2763-04
doi:10.3969/j.issn.1001-3695.2013.09.051

Research of quantitative network security assessment based on Bayesian-attack graphs

FANG Yan[1], YIN Xiao-chuan[1], LI Jing-zhi[2]
(1. *Dept. of Techniques of Command System Management, College of Information & Navigation, Air Force Engineering University, Xi'an* 710077, *China*; 2. *Xi'an Communication College, Xi'an* 710000, *China*)

Abstract: Aiming at solving the problems of attack graphs that the complicated relationships between nodes, the existing of cyclic attack paths and reflecting merely the static risk when evaluating the network security, this paper put forward the concept of Bayesian-attack graphs which simplified attack graphs and avoided the appearing of the cyclic paths by an optimized algorithm, combining attack graphs and Bayesian theory. By importing attack evidence and CVSS, this paper proposed a new method against to the vulnerability which could dynamically evaluate the whole and partial network security based on Bayesian-attack graphs. Experimental results in the real network show its veracity and validity, and the method can dynamically reflect the changes of the network security situation comparing to traditional assessment methods.
Key words: Bayesian-attack graphs; vulnerability; dynamic assessment; attack evidence

随着云计算等互联网服务技术的广泛应用,其面临的攻击威胁日益严峻。逐步呈现多样化、智能化的网络攻击不仅可以针对性地攻击网络系统内部组件的脆弱点,而且往往可以利用多个脆弱点以及设备的连接关系进行威胁渗透,对系统安全造成极大威胁,这就对网络安全分析提出了更高层次的要求。近年来逐渐发展成熟的脆弱性扫描技术(如 Nessus、X-Force 等工具)仅可以孤立地发现网络存在的脆弱点,而无法分析脆弱点之间的利用关系。攻击图作为一种网络脆弱性分析模型,从攻击者的角度出发,可以描述攻击者利用网络内部脆弱性间的关系进行状态的转换,从而综合分析网络面临的威胁。

1 相关研究

攻击图主要有状态攻击图[1]和属性攻击图[2]两类,状态攻击图中节点描述目标网络与攻击者的状态,但其存在状态爆炸等问题,近年来国内外学者倾向于用属性攻击图评估网络的安全状况。属性攻击图是一个有向图,展示了攻击者利用目标网络中脆弱点间的联系实施组合攻击的过程,它包含两类节点,即属性节点和原子攻击节点。为简化属性攻击图,渗透依赖攻击图与属性依赖攻击图的概念又被提出,然而两者在表现状态转换关系时无法完全还原属性攻击图的所有内容,具体应用中都存在局限性。在应用攻击图的研究方面,文献[3]提出了一种运用韦恩图解决攻击图中含圈路径的方法,提供了一种新的思路;文献[4]通过定义 n-有效路径在一定程度上简化了攻击图并避免了部分含圈路径的产生,但解决方案并不完善,且 n 的取值有待探讨;文献[5]提出了一种基于动态贝叶斯理论的网络安全评估方法,但其随时间推移需要维护的空间较大,实用性不强;文献[6]基于贝叶斯理论,通过定义的攻击图评估网络的安全,然而其对于原子攻击依赖关系仅考虑了"或""与"两种情况,忽略了两种关系混合出现的特殊情形;叶云等人[7]通过计算攻击图中节点的最大可达概率评估网络的安全状况,但并没有给出评定网络整体安全的方案;文献[8]以攻击图中漏洞间的依赖关系与 CVSS 评分为基础,计算网络的风险指数,但该方法仅从威胁发生可能性的角度出发,没有考虑网络的实时变化情况,缺乏动态的思想。

鉴于上述研究现状,本文基于贝叶斯攻击图(B-AG)提出了一种新的网络安全量化评估方法。

收稿日期: 2012-12-29; **修回日期**: 2013-01-30 **基金项目**: 国家自然科学基金资助项目(61272486)
作者简介: 方研(1989-),男(满族),辽宁宽甸人,硕士研究生,主要研究方向为网络与信息对抗(fangyan1989217@163.com);殷肖川(1961-),男,教授,主要研究方向为网络与信息对抗;李景志(1987-),男,硕士,主要研究方向为网络与信息对抗.

2 贝叶斯攻击图建模

2.1 贝叶斯攻击图定义

定义贝叶斯攻击图为一个四元组 B-AG = (S,A,e,P)。其中，S 为状态节点集合，A 为原子攻击集合即为有向边集合，e 为依赖关系集合，P 为概率集合。且 B-AG 需要满足下述条件：

a) $A \in S \times S$。$\forall a \in A, a = \text{pre}(a) \rightarrow \text{post}(a)$，$\text{pre}(a)$ 为 a 的起始状态节点，$\text{post}(a)$ 为 a 的目的状态节点。

b) $S = S_o \cup S_{in} \cup S_f$。$\forall S_i \in S, S_i$ 具有二态性，即 $S_i = 0$ 或 $S_i = 1$。$\forall S_i \in S_o$，不存在 $a \in A$ 使 $S_i = \text{post}(a)$；$\forall S_i \in S_{in}$，$\exists a_j, a_k \in A$ 使 $S_i = \text{post}(a_j) = \text{pre}(a_k)$；$\forall S_i \in S_f$，不存在 $a \in A$ 使 $S_i = \text{pre}(a)$。

c) $\forall S_i \in S, P(S_i)$ 表示状态 S_i 的可达概率，即 $S_i = 1$ 的概率；$\forall a \in A, P(a)$ 为原子攻击成功的概率，即从状态 $\text{pre}(a)$ 转移到状态 $\text{post}(a)$ 的概率。

d) $\forall S_i \in S_{in} \cup S_f, \exists e_i \in e$ 与 S_i 相对应，且 $e_i \in \{\text{AND}, \text{OR}, \text{MIX}\}$。在属性攻击图中原子攻击节点的父节点存在“与”关系，状态节点的父节点存在“或”关系。由于 B-AG 将属性攻击图中的原子攻击与有向边进行了合并，在 B-AG 中就可能出现三种依赖关系，即 AND、OR、MIX，为此在 B-AG 中用集合 e 进行定义，三种关系的基本模型如图 1 所示。

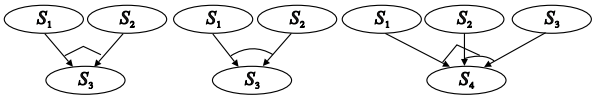

图1 基本依赖关系图

2.2 攻击图优化

贝叶斯理论与攻击图结合所面临的问题是，贝叶斯理论适用于有向无环图，而攻击图分析中却可能出现环路即含圈攻击路径，这对于网络安全的分析尤其是概率的计算造成了很大的影响。攻击图中的环路主要分为两种，即实际网络攻击实施过程中可能出现的环路和不可能出现的环路。如图 2(a) 中，椭圆表示状态节点，矩形表示原子渗透攻击，则在攻击路径 $a_6 \rightarrow S_6 \rightarrow a_7 \rightarrow S_7 \rightarrow a_6$ 中，原子攻击 a_6 与状态节点 S_7 的依赖关系存在矛盾，该多步攻击在实际网络中不可能发生，但却存在于攻击图中；而攻击路径 $S_4 \rightarrow a_4 \rightarrow S_5 \rightarrow a_5 \rightarrow S_4$ 虽然在理论上可能发生，但根据单调性假设[9]，即攻击者在攻击过程中不断地扩大自己的能力而不会失去已有的能力，所以攻击者重复获取已有权限不符合利益最大化原则。

为解决上述问题，本文提出一种攻击图优化算法，避免了上述情形中含圈路径的产生。其基本思想如下：为原始攻击图中的每一个原子攻击维护一个条件数组，对定义的可达状态队列 Q 进行出队操作，把依赖于出队状态的原子攻击的条件数组相应项做满足标记，当原子攻击所有初始条件状态都满足时，如果其不在原子攻击集合 A' 中，则将该原子攻击加入 A'，如果原子攻击实施后的可达状态不在状态集合 S' 中，则将其加入 S'，并且加入队列 Q。算法描述如下：

```
input: 攻击图;
output:可达状态集合 S', 原子攻击集合 A'。
initQueue(Q);
foreach S_i ∈ S_o do
    enQueue(Q, S_i);
    add_to(S', S_i);
endfor;
foreach a_i ∈ A do
    foreach q_j ∈ pre(a_i) do
    a_i.pre[q_j] = 0;
    endfor;
endfor;
while emptyQueue(Q) = 0 do
    q = deQueue(Q);
    foreach a_i ∈ post(q) do
    a_i.pre[q] = 1;
    if ∀q_j ∈ pre(a_i), a_i.pre[q_j] = 1 then
      foreach S_k ∈ post(a_i) do
        if S_k ∉ ancestor(pre(a_i)) ∪ pre(a_i) then
        if S_k ∉ S' then
          enQueue(Q, S_k);
          add_to(S', S_k);
          endif;
          if e_i ∉ E' then
          add_to(A', a_i);
          endif;
      endif;
      endfor;
    endif;
    endfor;
endwhile;
```

图 2(b) 为属性攻击图(a) 对应的 B-AG 的例子，对比发现 B-AG 相比属性攻击图在节点数量上进行了简化，状态间的转换关系更加清晰，便于分析。

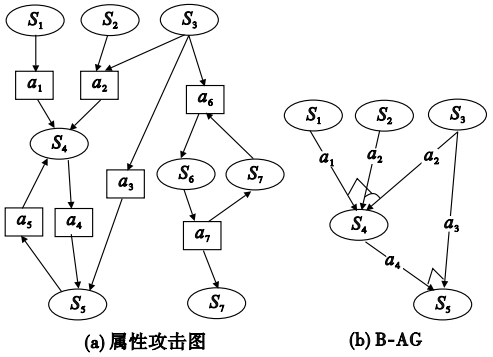

图2 实例对比图

2.3 节点概率计算

为评估网络安全状况，需要求出 B-AG 中各状态节点的可达概率，即 $P(S_i)$ 的大小。$\forall S_i \in S_o, S_i$ 为攻击的起始状态，理想情况下，一般 $P(S_i) = 1$。

$\forall S_i \in S_{in} \cup S_f$，根据贝叶斯理论可得

$$P(S_i) = P(S_i \mid Pa(S_i), Pa(S_i) \rightarrow S_i) \tag{1}$$

即 B-AG 状态节点的概率与其父节点和父节点到自身的原子攻击有关。由于父节点与子节点存在 AND、OR 和 MIX 的关系，将 $P(S_i)$ 定义为

$$P(S_i) = \begin{cases} \prod_{S_j \in Pa(S_i)} P(S_j) \times P(Pa(S_i) \rightarrow S_i) & e_i = \text{AND} \\ 1 - \prod_{S_j \in Pa(S_i)} (1 - P(S_j) \times P(S_j \rightarrow S_i)) & e_i = \text{OR} \\ 1 - \prod_{k=1}^{K} (1 - \prod_{S_j \in Pa(S_i)_k} P(S_j) \times P(Pa(S_i) \rightarrow S_i)) & e_i = \text{MIX} \end{cases} \tag{2}$$

假设图 1(a) 中状态 S_1、S_2 的可达概率分别为 0.7、0.8，原子渗透攻击 $S_1 \rightarrow S_3$、$S_2 \rightarrow S_3$ 概率分别为 0.6、0.5，由此可以计算出状态节点 S_3 的可达概率为

$$P(S_3) = P(S_1) \times 0.6 + P(S_2) \times 0.5 - P(S_1) \times 0.6 \times P(S_2) \times 0.5 = 0.652$$

由于网络环境的复杂性，对于网络安全评估需考虑其动态因素。随着时间的推移，网络系统可能已经搜集了部分或是全部的攻击行为，在这样的前提下，对于状态节点概率计算的准确性会降低。为此，本文引入证据 E 的概念，即为网络系统已观察到的渗透攻击行为或其使攻击者达到的状态。设 $E = \{S_1', S_2', \cdots, S_n'\}$ 为观察到的攻击者通过渗透攻击达到的状

态,则 $\forall S_i' \in E, S_i' = 1; S_i \in S - E$ 为概率有待确定的状态节点。运用贝叶斯理论的后验概率公式计算在已知证据的前提下状态节点 S_i 的可达概率为

$$P(S_i|E) = P(E|S_i) \times P(S_i)/P(E) \tag{3}$$

例如在图 1(a)中,假设网络管理员发现攻击者通过多步攻击到达状态 S_3 或监测到依赖于状态 S_3 的原子攻击发生,则可以认为 $S_3 = 1$ 为证据,即 $S_3 \in E$,此时可以通过贝叶斯推理更新 S_1 的可达概率为

$$P(S_1|S_3) = P(S_3|S_1) \times P(S_1)/P(S_3) =$$
$$(P(S_3, S_2|S_1) + P(S_3, \hat{}S_2|S_1)) \times P(S_1)/P(S_3) =$$
$$(P(S_3|S_2, S_1) \times P(S_2|S_1) + P(S_3|\hat{}S_2, S_1) \times P(\hat{}S_2|S_1)) \times$$
$$P(S_1)/P(S_3) = (P(S_3|S_2, S_1) \times P(S_2) +$$
$$P(S_3|\hat{}S_2, S_1) \times P(\hat{}S_2)) \times P(S_1)/P(S_3) = 0.816$$

同理可以更新 S_2 的可达概率。通过对比可以发现证据 $S_3 = 1$ 存在的情况下,S_1、S_2 的可达概率大于没有证据的情况,这与网络渗透攻击的实际情况相符。

3　网络安全量化评估

3.1　评估框架

根据网络风险评估的三要素,即资产、脆弱性、威胁,将网络安全指数定义为 $R = f(V, M, P)$。其中,V 代表资产的价值,M 代表脆弱点如果被利用对于对应资产造成的影响度,P 代表威胁成功利用脆弱点的可能性。即网络系统的安全度由资产重要性、脆弱点造成的损失度、威胁发生的概率这三点共同决定。

根据上述评估要素,本文建立如图 3 所示的总体评估框架,首先通过网络系统的资产信息及专家知识进行资产识别,即对关键资产的价值进行评分;其次以网络固有安全措施、网络资产、脆弱点及其 CVSS 评分为依据,进行脆弱性及威胁识别,即对脆弱点被利用造成的影响度及威胁利用脆弱点的可能性进行量值计算,并构建贝叶斯攻击图;在此基础上,结合网络在一定时间内搜集到的攻击证据通过具体的量化算法对网络的安全状况进行量化评估。

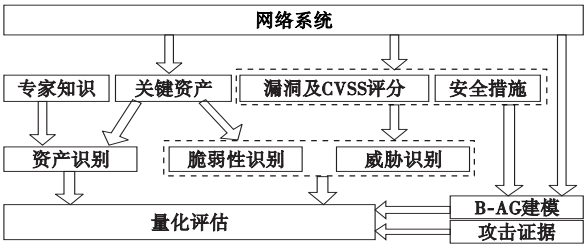

图3　基于B-AG的网络安全量化评估框架

3.2　安全指数量化

国家信息安全风险评估标准[10]指出,资产价值应根据资产在机密性、完整性和可用性的赋值等级,经过综合评定得出。本文根据国家标准将机密性、完整性、可用性分别分为很低、低、中等、高、很高共五个等级,等级赋值依次为 1 ~ 5,即等级越高代表机密性、完整性、可用性越强。通过专家打分的方式为三个指标赋值。由于脆弱性及威胁在网络环境中的复杂性、多样性,专家打分的方法会影响其准确度,本文参考了 CVSS 标准为这两方面进行赋值。CVSS 是由美国国家基础设施顾问委员会 NIAC 提出的,旨在提供一套开放的通用的脆弱点评分框架机制。CVSS 利用基本、时间和环境三个度量组计算脆弱点分数[11]。作为辅助度工具,时间与环境度量组不可控因素影响较大,本文在对脆弱点评分时暂不考虑这两个因素。基本度量组包含六项指标:入侵途径 AV、身份认证 AU、攻击复杂度 AC、机密性影响 CI、完整性影响 II、可用性影响 AI,各指标度量值如表 1 所示。

表 1　CVSS 基本度量组指标量值

指标	等级一	等级二	等级三
AV	本地(0.395)	邻近(0.646)	远程(1.0)
AU	多重(0.45)	单一(0.56)	无须(0.704)
AC	高(0.35)	中(0.61)	低(0.71)
CI /II /AI	无(0)	局部(0.275)	根本(0.66)

由表 1 可以看出,脆弱点对入侵途径即攻击位置要求越低、对攻击者身份认证要求越低、对攻击的复杂度要求越低,相应指标度量值越大,原子攻击成功的概率越大。因此,本文选取入侵途径、身份认证和攻击复杂度作为原子攻击节点自身概率计算的指标,定义原子攻击成功概率为

$$P(a) = AV \times AU \times AC \tag{4}$$

$P(a)$ 仅仅反映了原子攻击自身成功的概率,而在攻击图所描述的多步攻击中,原子攻击的成功执行还需依赖于其起始状态节点的可达概率。由于原子攻击可能会依赖多个状态节点,即 B-AG 中的 AND 关系,结合式(1) ~ (3)定义的状态节点的可达概率,将原子攻击的可达概率 $P'(a)$ 定义为

$$P'(a) = \begin{cases} P(a) \times \prod_{S_i \in \mathrm{pre}(a)} P(S_i) & \exists S_i \notin S_0 \\ P(\mathrm{post}(a)) & \mathrm{pre}(a) \subset S_0 \end{cases} \tag{5}$$

基本度量组中机密性、完整性、可用性影响越大,相应指标度量值越大,对于资产造成的破坏性也越大。由此将 CI、II、AI 分别与资产的机密性、完整性、可用性等级赋值相结合,得出脆弱点被利用后对资产造成的影响函数定义为

$$\mathrm{In}(a) = \log_2 \frac{(\alpha \times 2^{CI \times C} + \beta \times 2^{II \times I} + \gamma \times 2^{AI \times A})}{3} \tag{6}$$

其中:C、I、A 分别为专家对资产的机密性、完整性、可用性的赋值;α、β、γ 分别为机密性、完整性、可用性在资产中所占的权值,且 $\alpha + \beta + \gamma = 3$。而原子攻击安全指数可表示为原子攻击可达概率与其影响函数的乘积:

$$\mathrm{risk}(a) = P'(a) \times \mathrm{In}(a) \tag{7}$$

为把握网络系统整体的安全状况,定义目标网络总体安全指数为攻击图中所有原子攻击的风险指数的总和,即

$$\mathrm{risk}_{\mathrm{all}} = \sum_{a \in A} (P'(a) \times \mathrm{In}(a)) \tag{8}$$

4　实验分析

为了验证评估方法的可行性、有效性,搭建了图 4 所示的小型实验环境,主要分为攻击区与目标网络两部分。目标网络有 A、B、C 三台服务主机。其中,A 提供 Web 服务;B 提供 FTP、RSH 服务;C 提供 FTP、SSH、RSH 服务。防火墙配置规则为:允许 0 网段、2 网段访问 1 网段内的 80 端口,即 Web 服务;1 网段可以访问 2 网段的 21、22、514 端口,即 FTP、SSH、RSH 服务;其他的访问请求均被禁止。

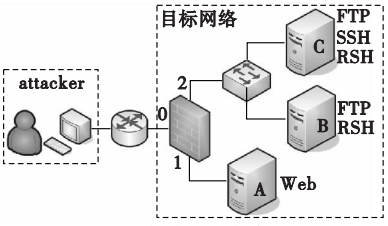

图4　实验网络拓扑图

首先运用 Nessus 对目标网络中的主机进行脆弱点检测,对

检测到的脆弱点信息进行汇总,结合防火墙的配置规则提取出可能被利用的脆弱点,并进行 CVE[12] 标志。由于本文主要考察脆弱点对网络服务造成的影响,所以对扫描得到的脆弱点所对应服务资产的机密性、完整性、可用性进行专家打分,赋权值 α、β、γ 分别为 1.1、1.0、0.9,以脆弱点的 CVE 编号为依据在 CVSS 评分系统查询各脆弱点基本度量组的分值,根据式(4)(6)可以得到 $P(a)$、$\ln(a)$。表 2 给出了检测到的可能被利用的脆弱点详细列表以及脆弱点所对应服务资产价值的专家赋值。

表 2 脆弱点相关信息列表

脆弱点名称	CVE 编号	对应服务	C	I	A
IIS bufferoverflow	CVE-2009-1012	A:Web	2	3	3
FTP rhost overflow	CVE-2011-4800	B:FTP	4	3	4
RSH login	CVE-2006-0408	B:RSH	3	3	4
RSH login	CVE-2006-0408	C:RSH	4	4	5
FTP rhost overflow	CVE-2011-4800	C:FTP	3	4	4
SSH buffer overflow	CVE-1999-1455	C:SSH	4	4	3

根据实验网络的具体拓扑、安全措施及脆弱点情况,得到经过优化后的贝叶斯攻击图,如图 5 所示。

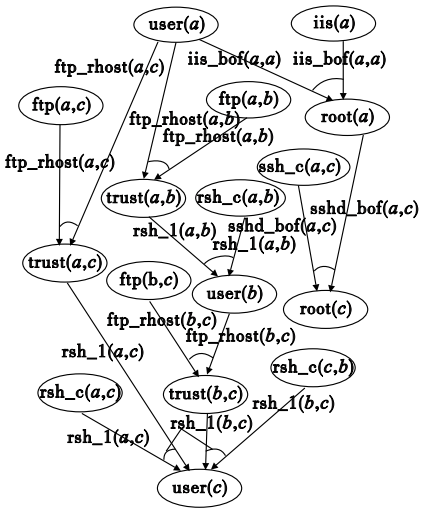

图5 实验网络对应的B-AG

根据贝叶斯攻击图中所展示的脆弱点利用关系及已得出的原子攻击成功概率 $P(a)$,运用式(1)(2)(5)计算出不考虑证据的情况下各状态节点的可达概率 $P(S_i)$ 及原子攻击的可达概率 $P'(a)$。利用攻击主机对目标网络进行针对性攻击,第一个时段内在服务主机 A 的日志中发现有非法的 root 操作,证明攻击者通过渗透攻击取得了服务主机 A 的 root 权限,即 $\text{root}(a)=1$ 为证据。随后,在时段 2 及时段 3 内又分别发现证据 $\text{user}(b)=1$、$\text{user}(c)=1$。根据式(3)(5)更新贝叶斯攻击图中状态节点及原子攻击节点的可达概率。最后运用式(7)(8)分别对无证据及有证据的三个时段中的原子攻击及网络整体安全指数进行量化计算,结果如表 3 所示,其中时段 0 表示无证据情况。

通过实验结果数据可以看出,由于主机 A 中 Web 服务对外网开放,资产价值不是很高,所以在时段 1 发现攻击者取得主机 A 的 root 权限后安全指数的增幅不大。时段 2、3 中陆续发现服务主机 B、C 被攻击侵入,由于 B、C 不对外网开放服务,说明攻击者成功实施了多步攻击,加之 B、C 中服务资产价值较大,原子攻击及网络总体的安全指数上升明显,表明网络被破坏程度加大。

上述实验结果与本文评估方法的理论相符,证明了方案不仅能够评估网络面临的潜在威胁,而且能够正确反映网络安全的态势变化情况,达到了动态评估网络整体及局部安全状况的目标。

表 3 安全指数量化表

攻击	时段 0	时段 1	时段 2	时段 3
iis_bof(a,a)	0.885 5	1.771 0	1.771 0	1.771 0
ftp_rhost(a,b)	0.974 9	0.974 9	2.452 0	2.452 0
rsh_c(a,b)	0.271 6	0.271 6	2.115 0	2.115 0
ftp_rhost(b,c)	0.158 9	0.158 9	1.237 3	2.110 2
rsh_c(b,c)	0.040 1	0.040 1	0.312 2	0.532 4
ftp_rhost(a,c)	1.237 3	1.237 3	1.237 3	2.110 2
rsh_c(a,c)	0.312 2	0.312 2	0.312 2	0.532 4
sshd_bof(a,c)	0.255 8	0.511 5	0.511 5	0.511 5
网络总体	4.136 3	5.277 5	9.948 5	12.134 8

5 结束语

安全评估一直是网络领域研究的热点,攻击图作为一种有效的分析方法,国内外学者不断提出新的见解。本文为简化攻击图的表达方式,提出了 B-AG 的概念,在此基础上建立了一种面向脆弱点的网络安全动态评估模型,并通过实验进行了可行性证明,为评估方法的研究提供了一种新的思路。下一步工作将进一步优化贝叶斯攻击图,提高其在大规模网络中应用的效率,并加强对攻击行为的预测分析,寻找代价最小的防护方案。

参考文献:

[1] SHEYNER O, HAINES J, JHA S, *et al*. Automated generation and analysis of attack graphs[C]//Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Sciety, 2002: 273-284.

[2] WANG Ling-yu, YAO Chao, SINGHAL A, *et al*. Interactive analysis of attack graphs using relational queries[C]//Proc of the 20th Annual IFIP Working Conference on Data & Applications Security. 2006: 119-132.

[3] WANG Ling-yu, ISLAM T, LONG Tao, *et al*. An attack graph-based probabilistic security metric [C]//Proc of the 22nd International Fede-ration for Information Processing. Berlin: Springer-Verlag, 2008: 283-296.

[4] 陈锋,张怡,苏金树,等. 攻击图的两种形式化分析[J]. 软件学报,2010,21(4):838-848.

[5] FRIGAULT M, WANG Ling-yu. Measuring network security using dynamic Bayesian network[C]//Proc of the 4th Conference on Computer and Communications Security ACM Workshop on Quality of Protection. New York: ACM Press, 2008: 23-30.

[6] POOLSAPPASIT N, DEWRI R, RAY I. Dynamic security risk management using Bayesian attack graphs[J]. IEEE Trans on Dependable and Secure Computing, 2012, 9(1): 61-74.

[7] 叶云,徐锡山,贾焰,等. 基于攻击图的网络安全概率计算方法[J]. 计算机学报,2010,33(10):1987-1996.

[8] 张玺,黄曙光,夏阳,等. 一种基于攻击图的漏洞风险评估方法[J]. 计算机应用研究,2010,27(1):278-280.

[9] AMMANN P, WIJESEKERA D, KAUSHIK S. Scalable, graph-based network vulnerability analysis[C]//Proc of the 9th ACM Conference on Computer and Communications Security. New York: ACM Press, 2002: 217-224.

[10] GB/T 20984, 信息安全技术—信息安全风险评估规范[S]. 北京: 中国标准出版社, 2007.

[11] MELL P, SCARFONE K, ROMANOSKY S. The common vulnerability scoring system (CVSS) and its applicability to federal agency systems, NIST IR 7435[R]. Gaithersburg: U. S. Department of Commerce, 2007.

[12] CVE. Common vulnerabilities and exposures [EB/OL]. (2012-12-18)[2012-12-29]. http://www.cve.mitre.org/.