基于节点博弈漏洞攻击图的网络风险分析方法

张 健 王晋东 张恒巍 王 娜
(解放军信息工程大学 郑州 450001)

摘 要 鉴于当前的漏洞风险分析方法未考虑攻防双方的相互制约关系,尝试将博弈论引入漏洞攻击图的节点分析过程,提出了基于节点博弈漏洞攻击图的风险分析模型RAMVAG。在此基础上,提出一种基于连通矩阵的漏洞风险分析算法VRAA。算法建立了攻击图的连通矩阵,在分析信息系统漏洞的自身风险和传播风险的基础上,对漏洞全局风险进行综合评价,评价结果能够帮助管理者确定网络系统的关键漏洞。实例分析证明了模型和算法的有效性。

关键词 节点博弈,漏洞攻击图,漏洞风险,传播风险
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.09.032

Network Risk Analysis Method Based on Node-Game Vulnerability Attack Graph

ZHANG Jian WANG Jin-dong ZHANG Heng-wei WANG Na
(Information Engineering University, Zhengzhou 450001, China)

Abstract Due to the lack of considerations of mutual constraints between offensive and defensive vulnerability in the current risk analysis methods, this paper attempted to introduce game theory into the nodes analysis process, and the Risk Analysis Model based on node game Vulnerability Attack Graph was proposed. On this basis, a vulnerability risk analysis algorithm based on connection matrix was proposed. The algorithm builds connection matrixes of the attack graph, and evaluates the overall risk based on the analysis of self risk and transmission risk of information system vulnerabilities. The evaluation result can help the manager to determine the critical vulnerability. The example analysis proves the effectiveness of the model and algorithm.

Keywords Node game, Vulnerability attack graph, Vulnerability risk, Transmission risk

攻击图是由Cunningham[1]于1985年最早提出的,其认为攻击图是由各种通过物理的或者逻辑的方法相连的组件构成。攻击图能够把网络中的漏洞关联起来进行深入分析,从而获取网络中潜在的安全威胁,使安全管理人员能够直观地把握网络漏洞之间的关系。与针对孤立的漏洞进行扫描分析的方法相比,攻击图能更准确有效地评估网络或系统的安全。漏洞挖掘技术[2]能够发现网络系统存在各项漏洞,为漏洞攻击图的生成奠定了基础。对于攻击图在风险分析中的应用,王永杰等[3]介绍了利用攻击图模型方法分析计算机网络攻击行为的基本原理,给出了攻击图生成算法,研究了利用攻击图对网络系统安全性进行风险分析的方法。马俊春等[4]提出了基于攻击图的网络安全策略制定方法,把安全策略的制定问题转化为带有惩罚的非约束优化问题,以最小的成本保证目标网络的安全。何江湖等[5]提出了一种基于漏洞关联攻击代价的网络攻击图的自动生成算法,有效结合漏洞之间的相关性,科学地评估攻击代价。王会梅等[6]提出了扩展网络攻击图生成方法,并提出一种基于扩展网络攻击图的网络攻击策略生成算法。

博弈论逐渐成为在具有相互对抗特征的环境中有效的决策理论和分析工具,基于博弈论的漏洞风险分析能够综合考虑攻击方与防御方之间的矛盾关系,更准确地评价双方在漏洞节点博弈中的收益情况。姜伟等[7]将网络攻击者和防御者相互博弈的过程看成一种两种角色、非合作零和博弈,建立了一个攻防博弈模型ADG,提出了对双方收益的计算方法。林旺群等[8]通过"虚拟节点"将网络攻防图转化为攻防博弈树,并给出了分别适应于完全信息和非完全信息两种场景的攻防博弈算法。

本文面向网络漏洞安全问题,提出了基于节点博弈漏洞攻击图的风险分析模型(Risk Analysis Model based on node game Vulnerability Attack Graph, RAMVAG)。节点博弈漏洞攻击图利用CVSS评分计算漏洞之间的渗透概率,对节点博弈过程进行分析,根据博弈收益情况对每个节点被渗透之后的风险进行了量化,分析了漏洞导致系统风险的严重程度,并提出了一种漏洞风险评估算法。该方法能够客观、准确地计算出漏洞对整个网络具有的风险,安全管理人员可以根据漏洞的风险评价结果清楚地识别安全隐患,集中力量消除最具危害性的关键漏洞,提高了网络安全管理的效率。

到稿日期:2013-11-19 返修日期:2014-02-14 本文受国防预研项目资助。

张 健(1989-),男,硕士生,主要研究方向为风险分析、测评认证,E-mail:shadowwn@126.com;王晋东(1966-),男,硕士,教授,主要研究方向为风险分析、资源管理;张恒巍(1978-),男,博士,讲师,主要研究方向为体系对抗、需求分析;王 娜(1970-),女,硕士,副教授,主要研究方向为资源管理、可信计算。

1 漏洞攻击图

1.1 漏洞攻击图概念

信息系统漏洞之间有着大量的因果连通关系，攻击者可以利用已渗透的主机漏洞作为跳板发起下一轮攻击，直到达到攻击目标。

定义 1(漏洞攻击图) 漏洞攻击图以漏洞作为图的节点，以攻击路径作为有向边，因此漏洞攻击图是一个有向图 $AG=\{N,L\}$。其中 $N=(n_1,n_2,\cdots,n_m)$ 为漏洞集合，表示该网络存在的所有漏洞。其中入度为 0 的节点称为起始节点，出度为 0 的节点称为目标节点，入度和出度均不为 0 的节点称为过程节点。L 为有向边的集合，表示漏洞之间的利用关系。

1.2 漏洞节点

漏洞节点是漏洞攻击图的重要概念，表示各漏洞在信息系统中的逻辑位置。

定义 2(漏洞节点) 定义漏洞节点 $n_i=\{v_i,r_i,A_i,D_i,u_i\}$，其中 $i=\{1,2,\cdots,n\}$，n 为攻击图中节点的总数。v_i 代表节点对应的漏洞名称。一般来说，一个节点对应一个系统漏洞，包括物理、网络、系统、应用和管理等方面的脆弱性，是攻击者策略实施的基础。r_i 为该节点处的主机资产或系统资源，是攻击者和防御者希望获得或者保护的对象，是攻击者和防御者策略实施的现实条件。A_i 代表节点所面临的威胁，它是用来标识关键节点在一个关键节点中所面临的威胁类型，构成节点博弈中的攻击者策略集。D_i 代表该节点处的防御措施，构成防御者策略集。$u_i=(u_a(i),u_d(i))$ 为一个二元组，代表攻防双方分别在该节点的预期收益，即节点代表的事件完成后对系统造成的影响。

2 漏洞连通性分析

漏洞连通度表示攻击者利用一个漏洞攻击另一个漏洞的可能性，在评价漏洞连通度时，可以参考 CVSS 对漏洞的评分方式。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。其基本度量组包含 6 项指标：入侵途径 AccessVector(AV)、身份认证 Authentication(AU)、攻击复杂度 AccessComplexity(AC)、机密性影响 ConfImpact(CI)、完整性影响 IntegImpact(II)、可用性影响 AvailImpact(AI)。文献[6]中仅以其中的 AC 字段来表征攻击者渗透该漏洞的难易程度，本文通过定义有向边的 3 个性质充分利用 CVSS 的评价标准来对漏洞间连通度进行评价，如图 1 所示。

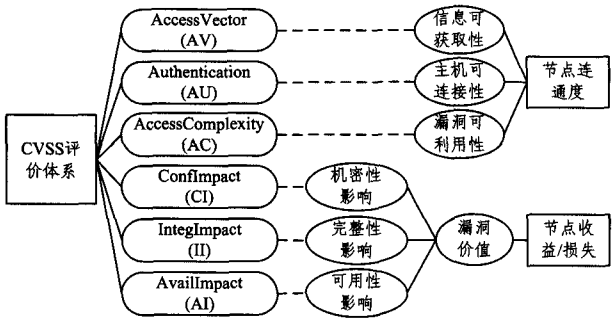

图 1 节点连通模型

定义 3(漏洞连通度) 在复杂的网络拓扑结构中，攻击者需要利用多个漏洞节点达到攻击目标，攻击者利用一个漏洞节点攻击另一个与该节点相邻接的脆漏洞节点的可能性称为漏洞连通度[9]。漏洞连通度与目标节点的信息可获取性、主机可连接性、漏洞可利用性相关。

信息可获取性以 NVD 数据库的 AccessVector 属性表示，参考 CVSS 其推荐分值为 0.395(local)，0.646(adjacent network)，1.0(Network)。

主机可连接性以 NVD 数据库的 Authentication 属性表示，参考 CVSS 其推荐分值为 0.45(multiple)，0.56(single)，0.704(none)。

漏洞可利用性以 NVD 数据库的 AccessComplexity 属性表示，CVSS 推荐分值为 0.35(high)，0.61(medium)，0.71(low)。

因此，节点 i 和节点 j 之间的连通度 p_{ij} 可表示为：

$$p_{ij}=\frac{AU}{AU+\sqrt{AC\cdot AV}}$$

其中，$p_{ij}\in(0,1)$，主机可连接性与漏洞连通度呈正相关关系，信息可获取性、漏洞可利用性与漏洞连通度呈负相关关系。一般来说，漏洞所在主机可连接性越强、信息获得越容易、漏洞利用难度越小，则攻击者有更大的概率选择攻击该漏洞，漏洞之间的连通度更大；如果攻击者难以通过主机认证、难以获取漏洞信息、漏洞利用难度大，则攻击者有较小的概率选择攻击该漏洞，漏洞之间的连通度较小。

3 节点风险分析

3.1 博弈模型建立

如果攻击方选择对节点进行渗透，则攻防双方在漏洞节点形成博弈局势。在节点博弈模型中，每个参与者都倾向于选择使自己的期望收益达到最大化的策略，最终各参与者会达到纳什均衡。此时，任何参与者改变其策略所获得的收益都不会大于均衡状态下的收益。

定义 4(节点博弈模型，Node Game Model，NGM) 攻击者和防御者在某个漏洞节点处的博弈模型可以用四元组 $G=(P,F,A,D)$ 来描述，其中 $P=(P_a,P_d)$ 为局中人的集合，其中 P_a 为针对某个攻击风险域的攻击者，P_d 为防御者。$F=(f_a,f_b)$ 为攻防双方依据各自策略竞争信息资源的收益函数。其中 f_a 是攻击者的收益函数，f_b 是防御者的收益函数。$A=\{A_1,A_2,\cdots,A_i,\cdots,A_m\}$ 为攻击者的攻击策略集(Attack Strategy Set，ASS)。$D=\{D_1,D_2,\cdots,D_j,\cdots,D_n\}$ 为防御者的防御策略集(Defense Strategy Set，DSS)。

根据英国标准协会(BSI)于 1995 年针对信息安全管理而制定的标准 BS7799，信息系统风险是指威胁利用信息系统的漏洞攻击资产而导致安全事件及其对系统的影响。攻击者总是试图利用该资产对象存在的漏洞来获得收益，在该节点处形成“威胁(Threat)-漏洞(Vulnerability)-资产(Asset)”风险链(Attack Chain)，节点模型如图 2 所示。

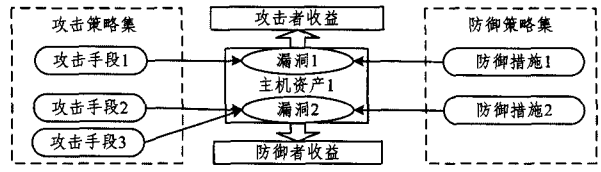

图 2 节点博弈模型

3.2 节点博弈分析

定义 5(攻击收益度) 防御收益度以 a_{ij} 表示,表示攻击者采用某攻击策略的有效程度,攻击收益度与防御手段的收益度密切相关。

定义 6(防御收益度) 防御收益度以 d_{ij} 表示,表示针对某一攻击所采取防御策略的有效程度。

攻击收益度和防御收益度的相互影响及评价标准如表 1 所列。

表 1 攻击收益度和攻防收益度评价

攻击收益度	防御收益度	描述
1	9	防御策略完全遏制了攻击策略,最大限度地保护了主机资产
3	7	防御策略有效遏制了攻击策略,保护了大部分主机资产
5	5	防御策略发挥了一定作用,保护了部分主机资产
7	3	防御策略的应用效果较弱,主机资产遭受了较大损失
9	1	防御策略对攻击策略基本没有效果,主机资产遭受严重损失

其中偶数评价表示对应不同评分等级的中间状态。$a_{ij}+d_{ij}=10$,该博弈为常和博弈,即攻防博弈是一个利益在攻击者和防御者之间转移的过程。攻击者和防御者采用手段的收益度可以组成 $m\times n$ 的收益矩阵,记为 M_a 和 M_d,如图 3 所示。

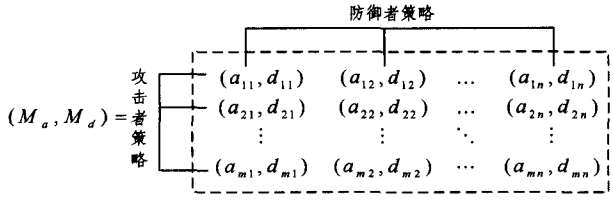

图 3 节点博弈收益矩阵

由于 a_{ij} 和 d_{ij} 的线性关系,因此只需要求解矩阵博弈 $\Gamma=(ASS,DSS,M_a)$ 的混合策略纳什均衡。设攻击者和防御者的混合策略为:

$$X=\{x=(x_1,x_2,\cdots,x_m)\mid\sum_{i=1}^{m}x_i=1,x_i\geqslant 0\}$$

$$Y=\{y=(y_1,y_2,\cdots,y_n)\mid\sum_{j=1}^{n}y_j=1,y_j\geqslant 0\}$$

攻击者的收益期望为 $u_a=\sum_{i=1}^{m}\sum_{j=1}^{n}a_{ij}x_iy_j$,防御者的收益期望为 $u_d=\sum_{i=1}^{m}\sum_{j=1}^{n}d_{ij}x_iy_j$。

对于双方来说,该收益期望值 u_a 和 u_d 越大越好。节点博弈总存在混合策略纳什均衡,即存在一组混合策略 $x^*=(x_1^*,x_2^*,\cdots,x_m^*)\in X$ 和 $y^*=(y_1^*,y_2^*,\cdots,y_m^*)\in Y$,使得该策略下攻防双方的收益大于其它混合策略。所以当且仅当双方的策略选择满足如下条件时,节点博弈达到均衡:

$$\begin{cases}\forall x,\sum_{i=1}^{m}\sum_{j=1}^{n}a_{ij}x_i^*y_j^*\geqslant\sum_{i=1}^{m}\sum_{j=1}^{n}a_{ij}x_iy_j^*\\ \forall y,\sum_{i=1}^{m}\sum_{j=1}^{n}d_{ij}x_i^*y_j^*\geqslant\sum_{i=1}^{m}\sum_{j=1}^{n}d_{ij}x_i^*y_j\end{cases}$$

将收益矩阵输入 Gambit 可得到攻击者和防御者关于该节点博弈的纳什均衡解 (x^*,y^*),计算漏洞节点 k 的双方节点博弈期望收益 $(u_a(k),u_d(k))$。系统损失 $\mu(k)$ 与防御者节点收益成反比,即 $\mu(k)=\frac{1}{u_d(k)}$。

综上所述,漏洞攻击图生成过程如下:

步骤 1 分析网络系统拓扑结构,使用漏洞扫描工具发现系统漏洞。

步骤 2 参照 CVE 建立漏洞之间的连通关系。

步骤 3 对有连通关系的两个漏洞,通过 CVSS 对其连通性进行评价,建立连通性邻接矩阵 M。

步骤 4 对每个节点进行博弈分析:

步骤 4.1 建立节点博弈模型。分析攻击策略集和防御策略集。

步骤 4.2 建立博弈收益矩阵。分析攻击策略和防御策略的收益度。

步骤 4.3 将收益矩阵输入 Gambit,得博弈矩阵的混合策略纳什均衡。

步骤 4.4 计算双方期望收益 $(u_a(k),u_d(k))$。

步骤 5 由节点间连通性和节点收益形成漏洞攻击图。

4 基于 RAMVAG 模型的漏洞风险

4.1 自身风险分析

借鉴人工免疫方面的知识和理论,定义漏洞的自身风险和传播风险概念,对漏洞的全局风险进行评价。

定义 7(漏洞风险) 漏洞风险 R_w 包括该漏洞的自身风险 R_s 和传播风险 R_o[10]。漏洞自身风险表示来自其它漏洞的威胁通过该漏洞所导致的系统风险,与其它漏洞与该漏洞的连通度、该漏洞的损失相关;漏洞传播风险表示漏洞通过有向边传递给其它漏洞的风险,与该漏洞与其它漏洞的连通度、其它漏洞的损失相关。漏洞全局风险为这两种风险的加权和:

$$R_w=R_s+R_o$$

定义 8(邻接矩阵[11,12]) 设 VAG 是由若干漏洞组成的漏洞攻击图,M 为 VAG 的邻接矩阵。则漏洞攻击图 VAG 和邻接矩阵 M 之间有以下特性:

(1)漏洞攻击图 VAG 和邻接矩阵 M 一一对应。

(2)邻接矩阵 M 中,如果有元素全为零的列,其所对应的节点为源节点或输入节点;如果有元素全为零的行,其所对应的节点称为汇点或输出节点。

(3)如果在漏洞攻击图 VAG 中,从 n_i 出发经过 1 条边可达到 n_j,则称 n_i 到 n_j 存在步长为 1 的通路,则此时矩阵 M 的第 i 行第 j 列元素为连通度 p_{ij},否则为 0。

漏洞邻接矩阵表示为:

$$M=\begin{bmatrix}p_{11}&p_{12}&\cdots&p_{1v}\\p_{21}&p_{22}&\cdots&p_{2v}\\\vdots&\vdots&\ddots&\vdots\\p_{v1}&p_{v2}&\cdots&p_{vv}\end{bmatrix}$$

其中,对角线上的 p_{ii} 均为零,v 为漏洞数,p_{ij} 为漏洞 n_i 和 n_j 之间的连通度。对矩阵 M 迭代相乘,可得漏洞之间的 r 阶连通矩阵为:

$$M^r=\begin{bmatrix}p_{11}^{(r)}&p_{12}^{(r)}&\cdots&p_{1v}^{(r)}\\p_{21}^{(r)}&p_{22}^{(r)}&\cdots&p_{21}^{(r)}\\\vdots&\vdots&\ddots&\vdots\\p_{v1}^{(r)}&p_{v2}^{(r)}&\cdots&p_{vv}^{(r)}\end{bmatrix}$$

其中,r 为邻接矩阵的阶,当 $r=2$ 时矩阵 M^2 中的元素表示距离为 2 的节点之间的连通度。则节点之间的连通矩阵为

$$M_0 = M^1 + M^2 + \cdots + M^n = \begin{bmatrix} \beta_{11} & \beta_{12} & \cdots & \beta_{1v} \\ \beta_{21} & \beta_{22} & \cdots & \beta_{2v} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{v1} & \beta_{v2} & \cdots & \beta_{vv} \end{bmatrix}$$

M_0 表示系统任意两个节点之间的连通度。攻击者会通过不同路径攻击漏洞，因此一个漏洞的自身风险可能来自于不同的风险源，节点 k 来自于源节点 l 的风险为：

$$R_s(l \to k) = \beta_{lk} \times \mu(k)$$

所有可能传播到节点 k 的风险即为该节点的自身风险：

$$R_s(k) = \sum_{l=1}^{v} R_s(l \to k) = \sum_{l=1}^{v} [\beta_{lk} \cdot \mu(k)]$$

则漏洞节点的自身风险向量为：

$$V(R_s) = [R_s(1) \quad R_s(2) \quad \cdots \quad R_s(v)]$$

4.2 传播风险分析

攻击者往往可以利用漏洞间的关系进行下一步攻击，因此用漏洞传播风险表示某个被渗透的漏洞传播到其它漏洞所造成的风险。张永铮等[13]提出由风险网络和风险传播算法构成的风险传播模型，本文则尝试利用 RAMVAG 模型的连通矩阵来对传播风险进行分析。

根据节点博弈结果，系统的漏洞风险向量为 $U = [\mu(1)\ \mu(2)\ \cdots\ \mu(v)]$。其中 v 为漏洞数，$\mu(k)$ 为第 k 个漏洞对系统造成的损失。漏洞 k 的传播风险向量为：

$$V(R_o)^{\mathrm{T}} = M_0 \cdot U^{\mathrm{T}}$$

$$= \begin{bmatrix} \beta_{11} & \beta_{12} & \cdots & \beta_{1v} \\ \beta_{21} & \beta_{22} & \cdots & \beta_{2v} \\ \vdots & \vdots & \vdots & \vdots \\ \beta_{v1} & \beta_{v2} & \cdots & \beta_{vv} \end{bmatrix} \begin{bmatrix} \mu(1) \\ \mu(2) \\ \cdots \\ \mu(v) \end{bmatrix} = \begin{bmatrix} R_o(1) \\ R_o(2) \\ \cdots \\ R_o(v) \end{bmatrix}$$

其中，$R_o(k) = \sum_{l=1}^{v} \beta_{kl} \times \mu(l)$ 为攻击者通过漏洞 k 对信息系统造成的传播风险。漏洞 k 对系统的全局风险向量为：

$$V(R_w)^{\mathrm{T}} = V(R_s)^{\mathrm{T}} + V(R_o)^{\mathrm{T}}$$

$$= \begin{bmatrix} R_s(1) \\ R_s(2) \\ \cdots \\ R_s(v) \end{bmatrix} + \begin{bmatrix} R_o(1) \\ R_o(2) \\ \cdots \\ R_o(v) \end{bmatrix} = \begin{bmatrix} R_w(1) \\ R_w(2) \\ \cdots \\ R_w(v) \end{bmatrix}$$

其中，$R_w(k)$ 为漏洞 k 的全局风险。

漏洞风险分析算法（Vulnerability Risk Analysis Algorithm，VRAA）

算法输入：漏洞邻接矩阵 M，防御者收益向量 U

算法输出：漏洞风险向量 $V(R_w)$

算法描述：

1. Begin
2. 初始化参数：
   $M[i][j] = p_{ij}$，$M_0[i][j] = [0]$，$SR = 0$；
   $V(R_s) = [R_s(1)\ R_s(2) \cdots R_s(v)] = [0]$；
   $V(R_o) = [R_o(1)\ R_o(2) \cdots R_o(v)] = [0]$；
   $V(R_w) = [R_w(1)\ R_w(2) \cdots R_w(v)] = [0]$；
3. For(i=1;i=i+1;i<=n)
4. $M^i = M^{i-1} \cdot M$；
5. $M_0 = M_0 + M^i$；
6. For(k=1;k=k+1;k<=v)
7. For(l=1;l=l+1;l<=v)
8. $R_s(l \to k) = \beta_{lk} \times \mu(k)$；
9. $R_s(k) = R_s(k) + R_s(l \to k)$；
10. $R_o(k \to l) = \beta_{kl} \times \mu(l)$；
11. $R_o(k) = R_o(k) + R_o(k \to l)$；
12. End
13. $R_w(k) = R_s(k) + R_o(k)$；
14. End
15. 输出 $V(R_w) = [R_w(1)\ R_w(2) \cdots R_w(v)]$；
16. End

5 实例分析

为说明 RAMVAG 模型在风险分析中的应用，建立图 4 所示的实验网络来进行漏洞风险分析，并相应提出基于 RAMVAG 模型的漏洞风险分析算法 VRAA。

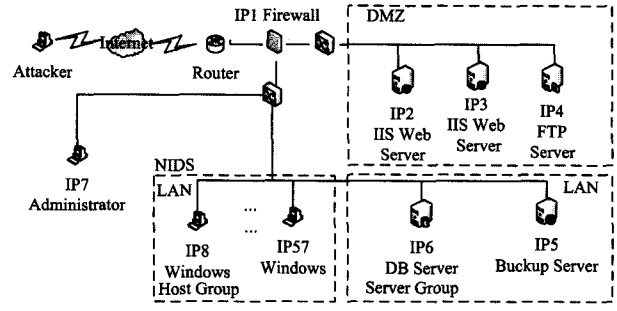

图 4 实验网络系统

实验网络系统共有 57 台网络设备，其中 DMZ 区域运行 3 台服务器，内部局域网分为两个部分：服务器组和用户组。服务器组包括备份服务器、数据库服务器和文件服务器。其中数据库服务器 IP6 上存储内部秘密数据，IP6 对 IP5 有信任关系，防火墙使外部主机只能访问 DMZ 区域的主机，DMZ 区域中 IP2，IP3 上的 WWW 服务可以向内网中的数据库服务器 IP7 读写数据，不能访问 LAN 内其它设备，IP4 可以访问 Host Group 中的任意主机。网络中各主机开放的服务及存在的漏洞如表 2 所列。

表 2 各节点上存在的漏洞及其访问关系

Host-ID	Service	Vulnerability-ID	Vulnerability Description	Result
IP1	None	12918	RedHat Linux Telnet Overflow	Root
IP3	IIS	4855	Unicode 漏洞	Root/DoS
IP6	Oracle	38115	Oracle 11gR2 远程命令执行漏洞	Root
IP7	None	6439	Weak Password	User
IP8－IP57	None	31874	Windows Server 服务远程 RPC 溢出漏洞	Root

分析表 2 所列漏洞之间的利用关系，其中由于 IP8－IP57 均为 Host 主机，因此仅以其中 IP8 的漏洞为例进行分析。参照 CVSS 评分标准，各漏洞之间有向边的属性值如表 3 所列。

表 3 有向边连通性的 CVSS 评价

ID	Access Vector	Authentication	Access Complexity	Connectivity
p_{12}	adjacent network	single	low	0.45
p_{13}	adjacent network	single	medium	0.47
p_{24}	adjacent network	multiple	high	0.54
p_{34}	network	multiple	high	0.43
p_{35}	network	multiple	high	0.43
p_{45}	local	multiple	high	0.55

则该网络系统的漏洞攻击图如图 5 所示。

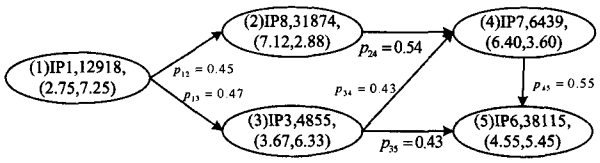

图 5　漏洞攻击图

对于节点博弈收益，以 IIS 服务器的 Unicode 漏洞为例，该漏洞的攻击手段有：(1)利用漏洞修改主页；(2)更改硬盘数据；(3)建立代理服务器。其防御手段主要有：(1)更改 Web 目录位置；(2)停止不必要的服务；(3)改变服务端口号；(4)限制 iusr_server 的权限。

通过咨询相关专家和历史数据对攻击收益度、防御收益度进行评价，可以获得该漏洞博弈的收益矩阵：

$$(M_a,M_d)=\begin{bmatrix}(2,8) & (4,6) & (8,2) & (5,5)\\ (7,3) & (5,5) & (6,4) & (1,9)\\ (4,6) & (9,1) & (8,2) & (2,8)\end{bmatrix}$$

将收益矩阵输入 Gambit 可得到节点博弈的混合策略为 $x^*=(\frac{2}{3},\frac{1}{3},0)$，$y^*=(\frac{4}{9},0,0,\frac{5}{9})$。攻防双方的期望收益为(3.67,6.33)。该漏洞攻击图所对应的邻接矩阵 M 为：

$$M=\begin{bmatrix}0 & 0.45 & 0.47 & 0 & 0\\ 0 & 0 & 0 & 0.54 & 0\\ 0 & 0 & 0 & 0.43 & 0.43\\ 0 & 0 & 0 & 0 & 0.55\\ 0 & 0 & 0 & 0 & 0\end{bmatrix}$$

VAG 中最大步长为 3，则对矩阵 M 进行两次迭代相乘，可得 M^2、M^3，则 $M_0=M+M^2+M^3$。

$$M_0=\begin{bmatrix}0 & 0.450 & 0.470 & 0.445 & 0.447\\ 0 & 0 & 0 & 0.540 & 0.297\\ 0 & 0 & 0 & 0.430 & 0.667\\ 0 & 0 & 0 & 0 & 0.550\\ 0 & 0 & 0 & 0 & 0\end{bmatrix}$$

漏洞风险向量 $U=[7.25\ 2.88\ 6.33\ 3.60\ 5.45]$，得到漏洞的自身风险向量和传播风险向量：

$V(R_s)=[0\ 1.30\ 2.98\ 5.09\ 10.69]$

$V(R_o)=[8.31\ 3.56\ 5.18\ 2.99\ 0]$

系统漏洞的全局风险向量：

$M(R_o)=[8.31\ 4.86\ 8.16\ 8.08\ 10.69]$

则漏洞的严重性程度为 $n_5>n_1>n_3>n_4>n_2$，n_5 和 n_1 漏洞对网络系统的影响最为显著。两者所对应的资产分别为 DB Server 服务器和网络防火墙，前者为数据库服务器，后者为网络进出的门户，其重要性在本算法中得以验证。这两个漏洞发生的风险往往会给网络系统带来难以挽回的重大损失，是管理者应该重点防御的关键漏洞。

结束语　综上所述，本文面向网络风险分析，主要介绍了节点博弈漏洞攻击图和一种漏洞风险分析算法，该模型和方法主要有以下几个特点和优势：

(1)尝试将博弈论引入攻击图节点分析。本文提出通过分析攻防双方博弈的混合策略纳什均衡，进而求得双方的收益期望来确定节点收益。文献[14,15]中将攻击结果划分为获得主机的 ACCESS、USER 或 ROOT 权限。相比上述文献，博奕论以收益度来评价结果，并在此过程中考虑攻防双方策略的制约关系，评价结果更加全面合理。

(2)提出通过 CVSS 评价体系对漏洞攻击图的节点连通度进行评价。合理借鉴了 CVSS 中 AV、AU 和 AC 3 个属性来对漏洞节点间的信息可获取性、主机可连接性和漏洞可利用性进行定量分析，提出了一种节点连通度的计算方法。相比文献[6,9]中给出的节点连通性量化方法，文中基于 CVSS 的量化方法更具权威性和可信性，更加简单方便。

(3)通过以上研究，提出一种基于节点博弈漏洞攻击图的风险分析模型 RAMVAG，通过漏洞攻击图建立网络系统漏洞之间的关系模型。

(4)在 RAMVAG 模型基础上提出了基于连通矩阵的漏洞风险分析算法 VRAA。将漏洞全局风险分为自身风险和传播风险，分别对其进行了分析计算。

参 考 文 献

[1] Cunningham W H. Optimal attack and reinforcement of a network [J]. Journal of the ACM, 1985, 32(3): 549-561

[2] 张友春，魏强，等. 信息系统漏洞挖掘技术体系研究[J]. 通信学报，2011，32(2)：42-47

[3] 王永杰，鲜明等. 基于攻击图模型的网络安全评估研究[J]. 通信学报，2007，28(3)：29-34

[4] 马俊春，王勇军，等. 基于攻击图的网络安全策略制定方法研究[J]. 高技术通讯，2012，22(4)：374-381

[5] 何江湖，潘晓中. 基于漏洞关联攻击代价的攻击图生成算法[J]. 计算机应用研究，2012，29(5)：1907-1909

[6] 王会梅，鲜明，等. 基于扩展网络攻击图的网络攻击策略生成算法[J]. 电子与信息学报，2011，33(12)：3015-3021

[7] 姜伟，方滨兴，等. 基于攻防博弈模型的网络安全测评和最优主动防御[J]. 计算机学报，2009，32(4)：817-825

[8] 林旺群，等. 基于非合作动态博弈的网络安全主动防御技术研究[J]. 计算机研究与发展，2011，48(2)：306-313

[9] 张永铮，方滨兴，等. 网络风险评估中网络节点关联性的研究[J]. 计算机学报，2007，30(2)：234-240

[10] 周亮，李俊娥，等. 信息系统漏洞风险定量评估模型研究[J]. 通信学报，2009，30(2)：71-76

[11] 叶云，徐锡山，等. 基于攻击图的风险邻接矩阵研究[J]. 通信学报，2011，32(5)：112-120

[12] 潘晓中，何江湖，等. 攻击图在风险评估中的矩阵可视化[J]. 小型微型计算机系统，2013，34(3)：553-556

[13] 张永铮，方滨兴，等. 用于评估网络信息系统的风险传播模型[J]. 软件学报，2007，18(1)：137-145