基于扩展网络攻击图的网络攻击策略生成算法

王会梅* 鲜 明 王国玉
(国防科技大学电子科学与工程学院 长沙 410073)

摘 要：该文针对网络攻防领域攻击策略生成问题的特性，从攻击者角度研究网络攻击图。根据漏洞信息对攻击模板进行实例化，维护原子攻击以及攻击的前提条件和攻击效果等因果关系，形成扩展网络攻击图，并进一步提出基于扩展网络攻击图的网络攻击策略生成算法，该算法能够动态的预测下一步网络攻击效果，求出达到该攻击效果的攻击链及其成功概率，为网络攻击过程的顺利实施提供决策支持。通过网络攻防实验，验证了网络攻击图的扩张和网络攻击策略生成算法的正确性。

关键词：网络攻击；攻击模板；扩展攻击图；攻击策略；效果预测
中图分类号：TP393.08 **文献标识码**： A **文章编号**：1009-5896(2011)12-3015-07
DOI: 10.3724/SP.J.1146.2011.00414

A Network Attack Decision-making Algorithm Based on the Extended Attack Graph

Wang Hui-mei Xian Ming Wang Guo-yu
(*College of Electronic Science and Engineering, National University of Defense Technology, Changsha* 410073, *China*)

Abstract: Considering the characteristics of attack decision-making issue in the domain of network attack and defense, the network attack graph model is extended from the view of attacker. Atomic attack is built by instantiating the attack pattern according the vulnerability. Maintaining the causality of precondition and effect condition of the atomic attack, therefore, the Extended Attack Graph (EAG) model is proposed. Furthermore, a network attack decision-making algorithm based on the extended attack graph is put forward; which can forecast attack effect dynamically and build the valid attack path and its occurrence probability through the in-depth analysis of the models' features. Through the network attack and defense experiments, the results show the completeness and soundness of the algorithm.

Key words: Network attack; Attack template; Extended attack graph; Attack strategy; Effect predict

1 引言

随着以平台为中心的计算向以网络为中心的计算转移，网络与信息安全的重要性不断凸现，网络入侵技术不断发展，网络攻击向大规模、协同化和多层次等方向发展，攻击行为表现出不确定性、复杂性和多样性等特点，网络攻防对抗已成为当前研究的热点。对网络攻击目标和攻击策略进行建模和推理可以在以下几个方面增强网络安全的防护水平。首先，在攻击发生前，可预测出攻击者最有可能采取的攻击策略，从而提高网络安全防护的针对性；其次在攻击过程中，及时检测到攻击事件，为采取适当应对措施争取时间。

网络攻击策略生成就是在当前取得的攻击效果和攻击目标信息的基础上，对网络攻击方案进行效果预测，并求出达到该攻击效果的网络攻击路径以及攻击成功概率，从而调整制定下一步的攻击策略，为网络攻击过程的顺利实施提供决策支持。目前国内外在此方面的相关研究成果主要是从防御者角度来对网络攻防过程进行分析的，比较有代表性的有：文献[1]在人工智能领域经典规划识别方法的基础上，提出了扩展目标规划图的网络攻击规划识别算法，但是该算法是从防护者角度针对入侵报警信息来识别网络攻击意图及规划。文献[2]研究了网络攻击条件下网络防御策略的制定问题。将网络攻击与防御看作一个博弈过程，通过求解博弈过程的纳什均衡来研究攻防双方的对抗策略和效用。文献[3]从防御的角度提出了网络防御图模型、攻防策略分类及其成本量化方法、网络攻防博弈模型和基于上述模型的最优主动防御选取算法。文献[4]提出了一种基于图模型的网络预测分析方法；构建了一个含有局部推理和全局推理两层推理的推理框架。文献[5]

2010-05-02 收到，2011-07-13 改回
国家自然科学基金(60372039)资助课题
*通信作者：王会梅 freshcdwhm@163.com

研究了网络攻击在线评估模型和评估算法，给出了网络攻击预测算法和攻击方案决策算法，但是该决策意见生成算法主要是决定当前是否停止攻击，并没有给出攻击决策方案。文献[6]提出了基于多准则决策模型的网络攻击评价方法，通过综合考虑攻击效果、攻击任务的攻击代价和攻击风险、攻击路径来选择最优策略。文献[7]提出了一种新的网络安全漏洞建模方法，在设计阶段来研究降低拒绝服务攻击对用户的影响的方法。

本文从攻击者角度出发，针对网络攻防领域攻击策略生成问题的特性，把攻击模板、攻击效果预测加入到网络攻击知识模型中，根据漏洞信息实例化攻击模板为具体的原子攻击，维护原子攻击以及攻击的前提条件和攻击效果等因果关系，形成扩展网络攻击图，并进一步提出基于扩展网络攻击图的网络攻击策略生成算法，采取前向搜索的方式和深度优先的搜索策略，求出达到该攻击效果的攻击链及其成功概率，从而指导网络攻击。通过网络攻防实验，验证了网络攻击图的扩张和网络攻击策略生成算法，证明了算法的有效性。

论文的结构安排如下：第 2 节介绍基于攻击模板库的网络攻击知识模型；第 3 节对扩展网络攻击图给出形式化定义；第 4 节描述基于扩展网络攻击图模型的攻击策略生成算法，并对算法的时间复杂性进行分析；第 5 节通过网络攻击实验来验证攻击策略生成算法；最后对全文进行总结，并给出进一步研究方向。

2 网络攻击知识模型

网络攻击主要是在掌握攻击目标足够多的信息以及漏洞的基础上，通过制定攻击策略，选择合适的时机进行攻击，同时根据攻击效果来调整下一步的攻击策略，使攻击达到最好。借鉴信号与系统中“系统是存在因果关系的整体”，研究如何有效地采用攻击模板对网络攻击知识进行建模和描述，并保证知识库构建的可行性、系统性以及可维护性。

参照文献[7,8]对攻击做如下假设：

(1)攻击者在实施网络攻击时，不断地向着增强自身对网络控制能力的方向改变网络和自身状态，这种攻击者能力不断增长的趋势，称之为单调性假设。

(2)只要存在通向攻击目标的攻击路径，攻击者通过足够的攻击代价最终可达到攻击目标。

(3)攻击过程中，攻击者总会选择付出代价最小但获取最大效能的攻击路径进行攻击，即攻击者是理性的。

定义 1 攻击模板 攻击者(针对系统或软件脆弱性)所采取的通用攻击手段的抽象描述，它包含一组可被实例化的局部变量，以 $AT = (\text{Name}, \text{Pre}, \text{Vul}, \text{Eff})$ 来表示。其中，Name 为攻击模板的名称；Pre 为利用攻击模板进行攻击所需的前提条件，一般包括：目标网络前提条件和攻击者能力前提条件。如目标主机上存在漏洞、攻击主机与目标主机存在 access 以上的访问关系等；Vul 为攻击漏洞，依附于攻击目标的运行服务、应用程序、操作系统等；Eff 表示利用攻击模板进行攻击取得的效果，描述了攻击成功后对网络和攻击者能力产生的影响，一般包括：目标网络影响和攻击者能力的影响，如源主机通过攻击对目标主机获取或提升权限。攻击者在实施网络攻击时，不仅会利用攻击目标网络中的漏洞对权限进行提升或进行拒绝服务攻击，同时也可通过实施正常网络操作达到攻击的目的。

本文采用的网络攻击知识模型的整体框架由图 1 所示。

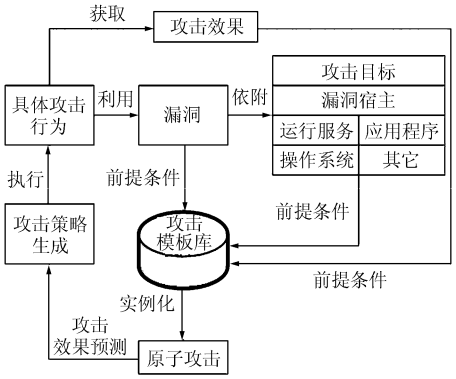


图 1 网络攻击知识模型

在攻击知识模型中，引入攻击目标、漏洞、具体攻击行为、攻击模板库、攻击效果和攻击策略生成来对攻击过程进行描述，同时引入以下特性对它们之间的关联关系进行描述：

(1)攻击模板库提前建立，在网络攻击过程中通过漏洞、攻击目标知识和已取得的攻击效果来实例化攻击模板生成原子攻击；

(2)引入攻击行为模型的层次结构，分别定义攻击模板库和具体攻击行为，同时具体攻击行为是某类攻击模板的实例化生成的原子攻击：

(3)在进行攻击策略生成时，根据攻击者的意图考虑当前实例化的原子攻击的预测攻击效果，争取以最小的攻击代价获得最大的攻击效果。

3　扩展攻击图的形式化定义

针对网络攻击效果及其攻击策略生成问题的复杂性，在提出的基于攻击模板的攻击知识模型的支持下，对攻击图进一步扩充，考虑原子攻击以及攻击的前提条件和攻击效果，形成扩展攻击图模型。

定义 2　扩展攻击图 EAG (Extended Attack Graph) 定义为 $\Gamma = \langle S, A, \delta, E, G \rangle$，其中 A 为原子攻击节点集合，其中每个元素表示为 $\text{attack}(a,i)$ (简记为 a_i)，a 为原子攻击实例，i 为一个时间戳(下同)，原子攻击可由攻击模板实例化生成。S 为状态节点集合，其中每个元素可表示为 $\text{state}(s,i)$ (简记为 s)，s 为一个状态实例。在每个原子攻击节点之前的状态节点为该原子攻击的前提条件；在每个原子攻击节点后的状态节点为该原子攻击的攻击效果，同时又可作为下一个原子攻击的前提条件。$\delta = (S \to \text{State}) \cup (A \to \text{AtomicAttack}) \cup (G \to \text{AttackGoal})$ 为标签函数。G 为攻击目标节点集合，其中每个元素表示为 $\text{goal}(g,i)$ (简记为 g_i)，g 为攻击目标实例。$E \subset ((S \times A) \cup (A \times S) \cup (S \times G))$ 为边集，包括以下几种不同类型的边：

$\text{pre-edge}(\text{state}(s,i), \text{attack}(a,j))$ $(i \le j)$：前提条件边，表示状态节点 $\text{state}(s,i)$ 是原子攻击节点 $\text{attack}(a,j)$ 的前提条件。

$\text{post-edge}(\text{attack}(a,i), \text{state}(s,i))$：攻击效果边，表示原子攻击节点 $\text{attack}(a,i)$ 发生后产生的攻击效果 $\text{state}(s,i)$。

$\text{goal-edge}(\text{state}(s,i), \text{goal}(g,i))$：目标描述边，表示状态节点 $\text{state}(s,i)$ 是目标节点 $\text{goal}(g,i)$ 的组成状态。

定义 3　攻击链　假设 a_i 和 a_j 是发生在时间 i 和 j 的两个原子攻击节点，定义 a_i 和 a_j 间存在攻击链当且仅当：$\exists s |\, \text{post-edge}(a_i, s) \wedge \text{pre-edge}(s, a_j)$，即 a_i 的某一攻击效果 s 是 a_j 的前提条件。在 a_i 和 a_j 之间存在一条 a_i 到 s 的攻击效果边，一条从 s 到 a_j 的前提条件边。

定义 4　因果链　假设 a_i 和 g_i 是发生在时间 i 的原子攻击节点和目标节点，定义 a_i 和 g_i 间存在因果关系链当且仅当 $\exists s |\, \text{post-edge}(a_i, s) \wedge \text{goal-edge}(s, g_i)$，即原子攻击 a_i 的某一攻击效果为目标 g_i 的描述。

4　基于扩展攻击图模型的网络攻击策略生成

在前面介绍的扩展攻击图的基础上，描述进行网络攻击时的策略生成算法。算法分为两步骤进行，首先为扩展网络攻击图的扩张过程，以前一攻击步骤取得的攻击效果、攻击目标信息以及网络攻击模板库为输入，根据漏洞信息对扩展网络攻击图进行预测扩张，从而构建前一步骤网络攻击结束后新的扩展网络攻击图；第二步骤为网络攻击策略生成算法，从新的扩展网络攻击图中分析预测攻击效果，从而给出攻击效益最大化的攻击策略。

扩展攻击图主要有两部分组成，一部分描述具体攻击行为、前提条件和实际攻击效果(用实线表示)，另一部分为执行每个具体攻击行为后，为了生成网络攻击策略而进行的网络攻击预测(用虚线表示)。

4.1 EAG 扩张算法

EAG 的扩张算法主要有两部分组成：原子攻击扩张和攻击目标扩张。原子攻击扩张根据前一攻击步骤的实际攻击效果和漏洞信息进行扩张，生成当前攻击步骤发生后新的扩张攻击图，扩张部分主要描述虚拟攻击过程，以便根据预测攻击效果进行攻击策略生成；攻击目标扩张阶段将预测攻击效果加入到目标节点。

原子攻击扩张算法以第 $i-1$ 个攻击步骤发生后产生的攻击效果、目标网络信息和攻击模板库为输入，算法首先根据攻击者获得的关于目标网络的漏洞信息 Vul_i，搜索攻击模板库确定可利用的攻击模板；根据漏洞 Vul_i 将相应攻击模板的相关变量进行实例化，得到原子攻击 a_{ij}，攻击前提条件 Pre_i 以及执行该原子攻击取得的攻击效果 Eff_i；通过迭代验证攻击前提条件 Pre_{ij} (j 为该原子攻击的前提条件个数)是否满足，如果满足则进行 EAG 的扩张，添加虚拟原子攻击和预测攻击效果节点，并添加预测前提条件边和预测攻击效果边，直到没有新的原子攻击添加到 EAG 中为止。

攻击目标扩张算法以原子攻击扩张后的扩展攻击图和新扩张的原子攻击的预测攻击效果 $\text{Eff}(a_{ij})$ 为输入，对每个预测攻击效果 $q_k \in \text{Eff}(a_{ij})$，如果拥有该状态节点的主机的权限最大，则添加预测目标节点和预测目标描述边；否则继续扫描 $\text{Eff}(a_{ij})$。具体算法如表 1 所示。

4.2 网络攻击策略生成算法

当前 EAG 扩展完成时，进入网络攻击策略生成阶段。网络攻击策略生成算法主要确定下一个攻击步骤需要采用的具体攻击行为，以其获得最大平均收益[9]。

为了确定条件节点和原子攻击节点在扩展攻击图中发生的概率，首先要获取条件节点和渗透节点的自身概率，然后再计算各个节点在攻击图中发生概率[10,11]。

表 1 扩展网络攻击图扩张算法

EAG Expansion

Input: $\Gamma_{i-1}=(S_{i-1},A_{i-1},\delta,E_{i-1},G_{i-1})$, $\text{Vuls}_{ij}(j=1,\cdots,m)$, AI_i, AT

Output: $\Gamma_i^{'}=(S_i^{'},A_i^{'},\delta,E_i^{'},G_i^{'})$

(1) Set $S_i^{'}=S_{i-1},G_i^{'}=G_{i-1}$

//原子攻击扩张

(2) For every $\text{Vuls}_{ij}\in\text{Vuls}_i$

(2.1) Instantiate AT with Vuls_{ij} to get a_{ij}, $\text{pre}(a_{ij})$ and $\text{Eff}(a_{ij})$

(2.2) For every $p_k\in\text{pre}(a_{ij})$ while $p_k\in S_i^{'}\cup AI_i$ Do

(2.2.1) Add a_{ij} to $A_i^{'}$ and set $\text{flag}(a_{ij})=0$

(2.2.2) If $p_k\in S_i^{'}$ Add $\text{pre-edge}(p_k,a_{ij})$

(2.2.3) If $p_k\in AI_i$ Add $\text{state}(p_k,i)$, $\text{pre-edge}(p_{ki},a_{ij})$ set $\text{flag}(p_{ki})=0$

(2.2.4) For every $q_k\in\text{Eff}(a_{ij})$

If $q_k\notin S'$ Add $\text{state}(q_k,i)$ to S' set $\text{flag}(q_{ki})=0$

Add $\text{post-edge}(a_{ij},q_{ki})$

//攻击目标扩张

(3) For every $\text{Eff}(a_{ij})$

(3.1) For every $q_k\in\text{Eff}(a_{ij})\ \forall q_k$, if $q_{ki}\cdot\text{host}=\text{host}(q_k)$, q_k pri$>q_{ki}\cdot$pri then

(3.1.1) If $q_k\succ G_{i-1}$

(3.1.1.1) If $q_k\succ G_i^{'}$ Add $\text{goal}(q_k,i)$ to $G_i^{'}$, Add $\text{goal-edge}(\text{state}(q_k,i)),\text{goal}(q_k,i)$ set $\text{flag}\ (\text{goal}(q_k,i))=0$

(3.1.1.2) If $q_k\in G_i^{'}$ Add $\text{goal-edge}(\text{state}(q_k,i),\text{goal}(q_k,i))$

(4) Return with $\Gamma_i^{'}=(S_i^{'},A_i^{'},\delta,E_i^{'},G_i^{'})$

对于针对漏洞的原子攻击节点，自身概率取自遵循 CVSS 标准的 NVD 数据库中的“Access Complexity”属性值 E[10]。NVD 数据库中的“Access Complexity”字段表征攻击者渗透该脆弱点的难易程度，即可视为成功执行该原子攻击的自身概率。按照 CVSS 的推荐，取值如下：

$$d(a_i)=\begin{cases}0.35, & \text{High}\\ 0.61, & \text{Medium}\\ 0.71, & \text{Low}\\ 0.71, & \text{Undefined}\end{cases}$$

对于非针对漏洞的攻击节点和条件节点，其自身概率可设为 1。

以扩展网络攻击图的虚拟攻击及预测效果部分为输入，采用回溯法来生成网络攻击链，通过计算每条攻击链的攻击成功的最大数学期望作为攻击策略生成的衡量标准。

首先生成网络攻击链，对于新生成的攻击目标节点 g_i，找到与 g_i 拥有目标描述边的状态节点，并添加到状态节点集合 N 中。对 N 中的每一个状态节点 s_i，采取前向搜索的方式和深度优先的搜索策略计算对于每一个状态 s_i 的攻击路径及其每条攻击路径的攻击成功概率，直到状态节点为预测攻击前的状态或当前攻击目标的信息即当前初始节点为止。

网络攻击策略生成算法如表 2 所示，攻击链获取算法如表 3 所示。

表 2 网络攻击策略生成算法

Attack Strategy

//扩展网络攻击图、原子攻击成功概率

Input: $\Gamma_i^{'}=(S_i^{'},A_i^{'},\delta,E_i^{'},G_i^{'}),D(A_i^{'})$

//攻击路径及其攻击成功率

Output: $P(G_i^{'}-G_{i-1})$, $D(G_i^{'}-G_{i-1})$

(1) For every $g_i\in G_i^{'}$ if $\text{flag}(g_i)==0$ then

(1.1) For every $s_i\in S_i^{'}\mid\exists\text{goal-edge}(s_i,g_i)$ $\text{enque}(N,s_i)$

(1.2) While $N\neq\varnothing$ do

(1.2.1) $n=\text{deque}(N)$

(1.2.2) $\text{obtain\_path}(n)$

(2) Return $P(G_i^{'}-G_{i-1})$, $D(G_i^{'}-G_{i-1})$

表 3 攻击链获取算法

Procedure $\text{obtain\_path}(n)$

(1) If $n\in S_{i-1}\cup AI_i$ Then

(1.1) Return $(P(n),D(n))=(P(n)\cup\{\perp\},1)$

(2) If $n\in S_i^{'}$ Then

(2.1) Get $a_i\in A_i^{'}\mid\exists\text{post-edge}(a_i,n)$

(2.2) $(P(n),D(n))=\text{obtain\_path}(a_i)$

(3) If $n\in A_i^{'}$ Then

(3.1) Get $p_i\in S_i^{'}\mid\exists\text{pre-edge}(p_i,a_i)$

(3.2) For every p_i Do

(3.2.1) $P(p_i)=\text{obtain\_path}(p_i)$

(3.2.2) $(P(n),D(n))=(P(n)\cup\{\rightarrow n\}\cup(P(p_1)\wedge\cdots\wedge P(p_t)),$ $D(n)\cdot\Pi D(p_i)$

4.3 扩展攻击图的调整

在执行每个具体攻击行为以后，首先需要对扩展攻击图进行调整，如果当前攻击成功，则把描述当前攻击的原子攻击节点、攻击状态节点、攻击目标节点以及它们之间连接边修改为实线，表明该攻击已经发生(flag=1)；把其它虚拟原子攻击节点、状态节点以及连接边删除；同时删除具有后续原子攻击节点的状态节点连接的目标节点和目标描述边。

4.4 算法分析

该算法主要包括扩展网络攻击图的扩张和网络攻击策略生成两部分。

定理 1　给定网络攻击图 $\Gamma_{i-1}=(S_{i-1},A_{i-1},\delta,E_{i-1},G_{i-1})$，漏洞个数 $V=\left|\{\text{Vuls}_{ij}\}\right|$，主机个数为 H，则扩展网络攻击图扩张算法的时间复杂度为 $O(VH^3)$。

证明　算法首先根据漏洞信息进行攻击模板的实例化，对于每一个漏洞，都要搜索模板库寻找相匹配的模板，最差情况为搜索完整个模板库，因此该阶段的时间复杂度为 $O(VT)$（T 为攻击模板的个数）；假设状态节点个数为 $N=\left|S_{i-1}\right|$，目标节点数位 $G=\left|G_{i-1}\right|$，假设实例化每个原子攻击 a_i 最多具有 C 个前提条件，即 $C=\text{Max}(\left|\text{Pre}(a_i)\right|)$，则实例化攻击模板和图的扩张阶段需要的时间复杂度为 $O(VC(N+M))$；最后为目标扩张阶段，需要的时间复杂度为 $O(VH^3)$。如果前一阶段扩展攻击图确定，则 $C(N+M)$ 为常数，因此扩展网络攻击图扩张算法的时间复杂度为 $O(VH^3)$。　　证毕

定理 2　给定扩展网络攻击图 $\Gamma_i^{'}=(S_i^{'},A_i^{'},\delta,E_i^{'},G_i^{'})$、预测原子攻击个数为 $n=\left|\{a_i^{'}\}\right|\ \left|a_i\in A_i^{'}\ \&\ \text{sign}(a_i)=0\right.$，与预测目标节点拥有目标描述边的状态节点个数为 $m=\left|\{s_i^{'}\}\right|\ \left|\exists\text{goal-edge}(s_i^{'},g_i^{'})\ \&\ g_i^{'}\in G_i^{'}\ \&\ \text{sign}(g_i^{'})=0\right.$ 假设每个原子攻击节点 $a_i\in A_i^{'}$ 最多具有 C 个前提条件，即 $C=\text{Max}\left(\left|\text{Pre}(a_i)\right|\right)\mid a_i\in A_i^{'}$，则计算可达网络攻击目标节点的攻击链及其成功概率算法的时间复杂度为 $O(mC^{n+1})$。

证明　对于算法 obtain_path(n)，若 n 为状态节点，由于在扩展网络攻击图生成时每一个原子攻击节点单独添加攻击效果节点，则它只有一个父节点，因此需要调用 1 次 obtain_path(n)；若 n 为原子攻击节点，则假设 $s_j\in\text{Pre}(a_i)$，其中 $0\le j\le C$，最多需要调用 C 次 obtain_path(n) 计算所有可达的攻击链。预测原子攻击节点个数为 n，因此攻击链的最大长度为 n，同时可生成 m 条攻击链，因此该算法的时间复杂度为 $O(mC^{n+1})$。　　证毕

5　应用实例

为了验证基于扩展攻击图模型的网络攻击策略生成算法的有效性和适用性，进行了网络攻击实验，实验网络拓扑图如图 2 所示。在实验过程中，通过本文提出的网络攻击策略生成算法来进行网络攻击规划。

为了描述方便，对攻击模式所需的谓词进行如表 4 所示的定义。

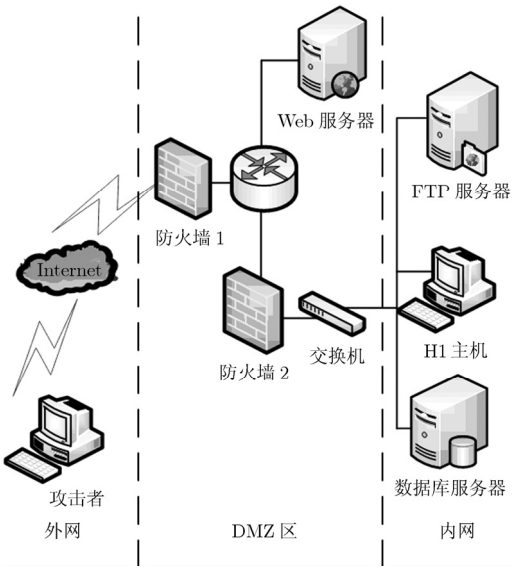


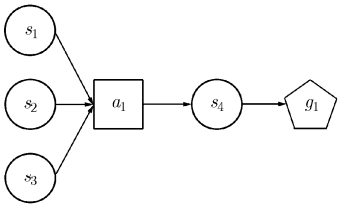
图 2 实验网络拓扑图

表 4 当前获取的目标网络信息

谓词	描述
Connection(Host1, Host2, Protocol, Port)	源主机 Host1 可通过协议 Protocol 访问目的主机 Host2 的端口 Port
RunService(Host, Service, Protocol, Port)	主机 Host 运行服务 Service，以协议 Protocol 提供服务并侦听端口 Port
RunSoftware (Host, Soft, Protocol, Port)	主机 Host 运行软件 Soft，以协议 Protocol 提供服务并侦听端口 Port
Vul(Host, Soft/Service, CVE)	主机 Host 上的服务或软件具有漏洞 CVE
RunCode(Host, Privilege)	攻击者可以在主机 Host 上以权限 Privilege 运行
DoS(Shosts, Dhost)	攻击者通过主机集 Shosts 对目标主机 Dhost 进行拒绝服务攻击
DoSE(Dhost)	Dhost 遭受拒绝服务攻击

攻击者(attacker)通过对目标网络进行信息搜集、勘察，发现目标网络的 Web 服务器运行 Apache，而该软件存在漏洞 CVE-2006-3747，从而利用该漏洞取得了目标网络 Web 服务器的控制权限。初始扩展网络攻击图如图 3 所示。

攻击者获取 Web 服务器控制权限后，通过信息勘察，得到如表 5 所示信息，其中脆弱点被成功利用的自身概率通过 NVD 数据库中的“Access Complexity”字段得到。



s_1: Connection(Attacker, WebServer, TCP, 80)
s_2: Vul(WebServer, Apache, CVE-2006-3747)
s_3: RunService(WebServer, Apache, TCP, 80)
a_1: R_b(Attacker, WebServer, Apache)
s_4: Runcode(WebServer, root)
g_1: Runcode(WebServer, root)

图 3 初始扩展网络攻击图

表 5 当前获取的目标网络信息

编号	获取的目标网络信息	脆弱点被成功利用的自身概率
1	RunService(WebServer, Apache, TCP, 80)	1
2	RunService(FTPServer, FTP, TCP, 21)	1
3	RunService(FTPServer, RPC, TCP, 135)	1
4	RunSoftware(H1, Microsoft IE, TCP, 80)	1
5	Connection(WebServer, H1, TCP, 80)	1
6	Connection(WebServer, FTPServer, TCP,21)	1
7	Connection(H1, FTPServer, TCP, 21)	1
8	Connection(H1, FTPServer, TCP, 135)	1
9	Vul(H1, Microsoft IE, CVE-2010-1259)	0.61
10	Vul(FTPServer, FTP, CVE-2008-0702)	0.61
11	Vul(FTPServer, RPC, CVE-2008-4250)	0.71
12	Connection(H1, DataServer, TCP, 1433)	1
13	Connection(H1, DataServer, TCP, 1433)	1

对网络攻击图进行扩展，形成如图 4 所示的扩展攻击图，图中节点的信息如表 6 所示。

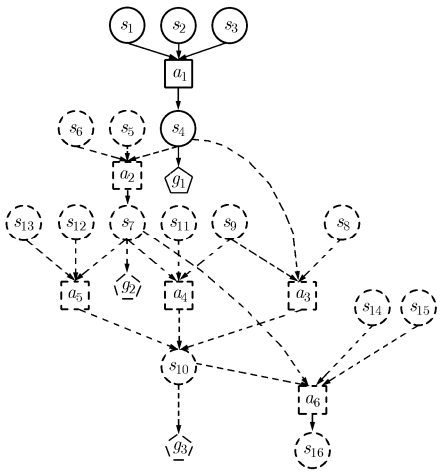


图 4 扩展网络攻击图

表 6 扩展攻击图中攻击节点的含义

节点	含义
a_1	R_b(Attacker, WebServer, Apache)
a_2	R_cr(WebServer, H1, IE)
a_3	R_b (WebServer, FtpServer, Ftp)
a_4	R_b (H1, FtpServer, RPC)
a_5	R_b (H1, FtpServer, Ftp)
a_6	DoS(H1, FtpServer, DataServer)
s_7,g_2	RunCode(H1, user)
s_{10},g_3	RunCode(FtpServer, root)
s_5,s_6	与表 2 第 5, 9 行相同
s_8,s_9	与表 2 第 6, 10 行相同
s_{11}–s_{13}	与表 2 第 7, 8 和 3 行相同
s_{14},s_{15}	与表 2 第 12 和 13 行相同
s_{16}	DoSE(DataServer)

根据攻击策略生成算法，可达目标节点 g_2，g_3 的攻击链：

$$P_{21}:\ \perp\rightarrow a_1\rightarrow a_2\rightarrow g_2$$
$$P_{31}:\ \perp\rightarrow a_1\rightarrow a_3\rightarrow g_3$$
$$P_{32}:\ \perp\rightarrow a_1\rightarrow a_2\rightarrow a_4\rightarrow g_3$$
$$P_{33}:\ \perp\rightarrow a_1\rightarrow a_2\rightarrow a_5\rightarrow g_3$$

各个攻击路径的攻击成功概率为 $D_1=p(a_1)\cdot p(a_2)=0.61$，$D_2=p(a_1)p(a_3)$=0.61，$D_3=p(a_1)p(a_2)\cdot p(a_4)=0.43$，$D_4=p(a_1)p(a_2)p(a_5)=0.37$。因此下一步可选择攻击链 P_{21} 和 P_{31} 进行攻击，可获取目标网络中 Ftp 服务器和用户 H1 的根用户权限。

原子攻击 a_6 为主机 H1 和 FtpServer 对 DataServer 实施的拒绝服务攻击。则 $D(a_6)$=$D(g_2)\cdot D(g_3)$，最大值为 $D(a_6)$=D_1D_2=0.37。

6 结束语

从攻击者角度对攻击图进行进一步扩展，根据漏洞信息实例化攻击模板为具体的原子攻击，维护原子攻击以及攻击的前提条件和攻击效果等因果关系，形成扩展网络攻击图，并进一步提出基于扩展网络攻击图的网络攻击策略生成算法。通过网络攻击实验验证，本算法具有：攻击模板知识库构建具有可行性、易维护性和可扩展性，对实际情况下网络攻击策略的生成具有更强的实用性优势；扩展网络攻击图的扩张是动态的，在每一步骤攻击完后，通过获取的攻击效果知识和攻击目标信息对扩张网络攻击图进行扩张；通过网络攻击策略生成算法可以更加快速有效地完成既定的攻击目标，避免冗余

攻击，从而减少攻击被检测和发现的可能性。

下一步的研究方向主要包括：(1)进一步完善攻击模板库，尽可能加入漏洞利用方法，从而能更加快速地实施攻击方案；(2)原子攻击成功概率的获取，对模板库中的原子攻击的成功概率进行网络攻防测试，提高其准确性。

参 考 文 献

[1] 诸葛建伟, 韩心慧, 叶志远, 等. 基于扩展目标规划图的网络攻击规划识别算法[J]. 计算机学报, 2006, 29(8): 1356–1366.
Zhuge J, Han X, Ye Z, *et al*.. A network attack plan recognition algorithm based on the extended goal graph[J]. *Chinese Journal of Computers*, 2006, 29(8): 1356–1366.

[2] Liu Peng, Zang Wan-yu, and Yu Meng. Incentive-based modeling and inference of attacker intent, objectives, and strategies [J]. *ACM Transactions on Information and System Security*, 2005, 8(1): 78–118.

[3] Jiang Wei, Fang Bin-xing, Zhang Hong-li, *et al*.. Optimal network security strengthening using attack-defense game model[C]. Proceedings of the 6th International Conference on Information Technology: New Generation ITNG 2009, Las Vegas, Nevada, USA, 2009: 475–480.

[4] Wang Wei and Daniels E. A graph based approach toward network forensics analysis [J]. *ACM Transactions on Information and System Security*, 2008, 12(1): 1–33.

[5] 王永杰, 江亮, 鲜明, 等. 网络攻击效果在线评估模型与算法研究[J]. 计算机科学, 2007, 34(5): 72–74.
Wang Yong-jie, Jiang Liang, Xian Ming, *et al*.. Research of online evaluation model and algorithm for network attack effect[J]. *Computer Science*, 2007, 34(5): 72–74.

[6] Wen Dan-yan, Ji Yi, Li Xiao-jian, *et al*.. A multiple criteria decision making model for CNO attack scheme evaluation[C]. International Conference on Computational Intelligence and Software Engineering, Wuhan, China, 2009: 1–7.

[7] Qiu Xiang-qun and Paterson R. An innovative network security vulnerability modeling method and tool[J]. *IEEE Communications Magazine*, 2010, 48(1): 104–108.

[8] Rodolphe O, Yves D, and Mohamed K. Experimenting with quantitative evaluation tools for monitoring operational security[J]. *IEEE Transactions on Software Engineering*, 1999, 25(5): 633–651.

[9] Kijsanayothin P and Hewett R. Analytical approach to attack graph analysis for network security[C]. International Conference on Availability, Reliability and Security, Krakow, Poland, 2010: 25–32.

[10] FIRST. Common vulnerability scoring system. http://www.first.org/cvss/, 2007, 6.

[11] 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.
Ye Yun, Xu Xi-Shan, Jia Yan, *et al*.. An attack graph-based probabilistic computing approach of network security[J]. *Chinese Journal of Computers*, 2010, 33(10): 1987–1996.

王会梅：女，1981 年生，博士生，研究方向为网络安全、电子信息系统建模仿真与评估.

鲜　明：男，1970 年生，研究员，博士生导师，研究方向为网络安全、电子信息系统建模仿真与评估、网电空间对抗.

王国玉：男，1962 年生，研究员，博士生导师，研究方向为信息对抗、目标识别、电子信息系统建模仿真与评估.