文章编号: 1001- 2486(2008) 02- 0097- 05

一种基于图论的网络安全分析方法研究*

张维明, 毛捍东, 陈 锋
(国防科技大学 信息系统与管理学院, 湖南 长沙 410073)

摘 要: 随着信息技术安全问题的日益突出, 对网络系统进行安全分析日益重要。提出了一种基于图论的网络安全分析方法 NEG- NSAM, 在进行网络参数抽象和脆弱性关联分析的基础上, 构造网络渗透图模型, 刻画了威胁主体逐步渗透安全目标的动态过程。针对大规模网络环境, 提出了渗透图简化算法。最后, 运用 NEG- NSAM 方法进行了实例分析, 验证该方法的可行性和有效性。

关键词: 安全分析; 网络渗透; 渗透图; 网络参数抽象
中图分类号: TP393. 08 文献标识码: A

Study on Network Security Analysis Method Based on Graph

ZHANG Wei-ming, MAO Han-dong, CHEN Feng
(College of Information System and Management, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: As information technology security issues become more prominent, the network system security analysis is becoming increasingly important. The paper presents NEG-NSAM, a network security analysis method. Based on network parameters abstract and vulnerability correlation analysis, the network exploitation graph model was constructed, and the dynamic process of a gradual infiltration of the main threats to security objectives was characterized. For large-scale network environment, the simplified algorithm of network exploitation graph model was proposed. Finally, the NEG-NSAM was used to exemplify the network and verify the feasibility and effectiveness of the method.

Key words: security analysis; network exploit; exploitation graph; network parameter abstract

目前, 关于基于模型的网络安全分析方法的研究还处于起步阶段, 尚未形成系统化的理论方法。主要的研究工作包括: Schneier 首先提出攻击树模型概念[1], 用 AND-OR 形式的树结构对攻击行为进行建模, 评估系统安全性, 但由于树结构的内在限制, 攻击树不能用于建模多重尝试攻击、时间依赖及访问控制等场景。Dacier[2] 和 Ortalo[3] 等运用权力提升图的概念, 利用通往攻击目标的不同路径表示攻击者的不同攻击过程, 以此反映出攻击者提升权限的过程, 并依据经验来计算入侵行为的平均攻击代价, 但该方法在计算平均攻击代价时缺乏理论基础。Swiler 等提出了一种攻击图模型[4], 在安全分析过程中考虑到了网络拓扑信息, 但其缺点是攻击图采用手工绘制, 无法适应中大规模网络环境。文献[5- 6] 使用改进的模型检测器(SMV/NuSMV) 来构建攻击图。文献[7- 16] 也对基于模型的网络安全分析方法进行了一定的研究。

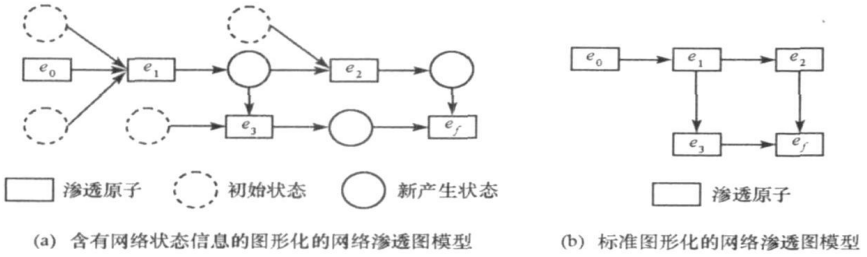
上述分析方法都是单一地从攻击者的角度来考虑问题, 而忽视了除了攻击者之外的其他一些导致网络系统安全性受损的因素, 如网络拓扑结构等, 不能很好地将系统脆弱性、网络拓扑结构、主机之间的信任关系、详细的系统配置信息、软件硬件的使用等信息融入到评估模型中。此外, 这些方法都不能适应中大规模网络系统, 随着规模的扩大, 算法可能会导致“状态爆炸”现象。针对上述问题, 本文提出一种基于渗透图模型的网络安全分析方法 NEG- NSAM, 在对网络系统参数进行抽象和对脆弱性进行关联分析的基础上, 构造网络渗透图模型, 从而分析可能入侵安全目标的渗透路径。

* 收稿日期: 2007- 08- 31
基金项目: 国家自然科学基金资助项目(70371008)
作者简介: 张维明(1962—), 男, 教授, 博士生导师。

1 网络渗透图模型的定义

文献[12]提出了渗透图(Exploitation Graph)的概念,文献[16]提出了渗透依赖图(Exploit Dependency Graphs)的概念,表示攻击者利用多个脆弱性的多阶段入侵过程。本文在此基础上提出了网络渗透图模型(NEG, Network Exploitation Graph model)的概念。

定义 1 $NEG=(E, S_p, S_d, S_f, L, EP)$ 为网络渗透图模型,其中, E 表示渗透原子集合, S_p 表示初始的网络状态集合, S_d 表示新产生的网络状态集合, S_f 表示渗透目标状态集合, L 为标签函数, EP 为渗透路径集合。图形化的 NEG 描述了威胁主体到达安全目标所有可能的渗透路径,其节点表示网络中存在的原子渗透,边表示随着渗透行为的发生所导致网络状态的变化(包括网络连接关系、访问权限等状态)。以渗透路径[e_0, e_1, e_2, e_f]和[e_0, e_1, e_3, e_f]为例,图 1(a)表示含有网络状态信息的图形化的网络渗透图模型;图 1(b)表示标准的图形化的网络渗透图模型。



(a) 含有网络状态信息的图形化的网络渗透图模型 (b) 标准图形化的网络渗透图模型

图 1 图形化的网络渗透图模型

Fig. 1 Graphical network exploitation graph model

NEG 满足如下属性:

(1) for $\forall c \in pre(e_1)$, $c \in S_p$, 表示渗透路径的第一个渗透原子的发生前提集合被 S_p 满足;

(2) $S_f \subset post(e_n)$, 表示目标状态集合一定包含于最后一个渗透原子的后果集合;

(3) if $i \neq j$, then $e_i \neq e_j$, 渗透路径中不存在重复的两个渗透原子,即遵循单调性假设;

(4) for $\forall c \in pre(e_i)$, $c \in \bigcup_{j=1}^{i-1} post(e_j) \cup S_p$, 表示威胁主体的状态在不断增加,即拥有的网络系统资源随着渗透深入在不断增加;

(5) $post(e_{i-1}) \cap pre(e_i) \neq \Phi (2 \leqslant i \leqslant n)$, 表示前一个渗透原子的后果集是为后一个渗透原子的成功发生创造条件;

(6) $S_f \subset S_p \cup S_d$, 表示原始事实集合和派生事实集合的并集为网络状态的总集合。

2 网络安全分析方法 NEG-NSAM

2.1 概要框架

根据本文第 1 节 NEG 的定义及其性质可知,网络渗透图模型 NEG 在融入网络系统多个数据源的基础上,NEG 能细致而全面地刻画出该特定威胁主体在初始网络系统安全状态下实现特定渗透目标的动态过程,即形式化地描述出特定威胁主体非法获取特定关键信息资产上的特定访问权限的安全风险的形成过程。本文提出一种基于 NEG 的网络安全分析方法 NEG-NSAM,图 2 给出了该方法的概念框架。

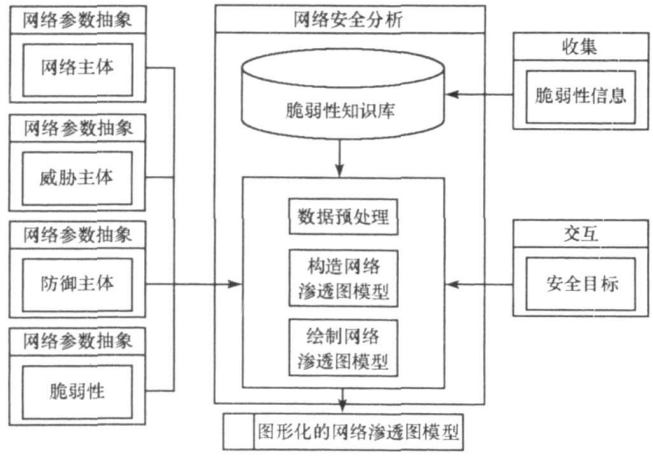


图 2 NEG-NSAM 方法的概念框架

Fig. 2 Conceptual framework of NEG-NSAM

从图 2 所示的概念框架可以看出, NEG- NSAM 方法由四个核心模块组成: 网络参数抽象、数据预处理、构造网络渗透图模型和绘制网络渗透图模型, 下面分别对每个核心模块进行阐述。

(1) 网络参数抽象。对网络系统中的网络主体、威胁主体、防御主体以及脆弱性等进行参数抽象, 为构建网络渗透图模型作好数据准备。

(2) 数据预处理。将获取的网络参数进行格式处理, 并将脆弱性信息转换为原子渗透集合。同时, 对冗余的原子渗透进行简化处理, 本文 2.3 小节详细介绍了网络渗透图模型简化算法 NEGSA。

(3) 构造网络渗透图模型。将格式化后的网络参数和脆弱性知识库作为输入, 利用网络渗透图构造算法, 生成网络渗透图模型。本文 2.2 小节讨论了构造网络渗透图模型的基本思想和算法。

(4) 绘制网络渗透图模型。图形化显示网络渗透图模型, 可以更加直观地反映当前的安全态势, 同时还可以运用图论的相关理论进行更加深入的安全性分析。

2.2 构造网络渗透图模型

网络渗透图模型描述了威胁主体利用系统脆弱性而导致系统状态发生转移的过程, 其构造的基本思想为: (1) 根据网络参数抽象和数据预处理的结果, 定义目标网络系统的原子渗透集合、初始状态集合。(2) 从系统初始状态出发, 在不同的原子渗透之间进行映射, 从而找出使系统状态发生变化的网络渗透行为。(3) 直到没有可用的行为使系统状态继续发生变化, 检查最终状态是否与威胁主体的目标相符合, 如果不符合, 则删除相关的系统状态和渗透行为。(4) 如果存在与威胁主体目标相符的情况, 剩余的状态和行为就构成了网络系统的渗透图模型。网络渗透图模型构造算法描述如下:

```
算法: 网络渗透图模型构造算法
BEGIN PROC
  假设 E_n 表示分层渗透图第 n 层的渗透原子集, C_n 表示第 n 层的系统状态。
  IF (S_0 = Φ) ∨ (S_f = Φ) ∨ (S_f ⊆ S_0) THEN
    EXIT;
  END IF
  E_0 = Φ; C_0 = S_0; n = 1
  REPEAT
    FOR EACH e_i ∈ E_n DO
      IF pre(e_i) ⊆ C_{n-1} THEN
        FOR EACH c_i ∈ post(e_i) DO
          标志 c_i 和 e_i 为第 n 层的状态和渗透
        END FOR
      END IF
    END FOR
    C_n = C_{n-1} + C'_n (C'_n 为第 n 层满足的状态)
    n = n + 1;
  UNTIL (|E| = n) ∨ (C'_n = Φ) ∨ (S_f ⊆ E_n)
END PROC
```

文献[15] 中采用系统状态作为节点, 构造了网络系统的攻击图模型。相对于基于状态的攻击图, 网络渗透图模型显得更加直观。同时, 网络渗透图模型的构造时间复杂度将会大大减小, 攻击图模型产生的时间复杂度为 $O(|C|^2|E|)$, 而渗透图模型产生的时间复杂度为 $O(|C||E|^2)$, 其中 $|E|$ 是原子渗透的个数, $|C|$ 是系统状态的个数, 通常情况下, $|C| \gg |E|$, 可以推出 $O(|C|^2|E|) \gg O(|C||E|^2)$。

2.3 网络渗透图模型简化算法 NEGSA

即使采用了合理的数据结构来描述原子渗透及其之间的关系, 但随着网络系统规模扩大, 原子渗透

数目急剧增长,网络渗透图模型也将急剧膨胀。复杂的网络渗透图模型不仅难于进行安全分析,其构造过程也相当耗时。

定义2 对于$\forall e_i \in E$,如果存在一个原子渗透e_j,使得同时满足:

(1)$pre(e_i) = pre(e_j)$,表示两个原子渗透的前提集相同;

(2)$S_f \subseteq (S_p \cup S_d) - post(e_i)$和$S_f \subseteq (S_p \cup S_d) - post(e_j)$同时成立,表示即使从原子渗透集合中抽取掉原子渗透$e_i$或者$e_j$,渗透目标仍能满足。

则称原子渗透e_i和e_j具有语义相似性,简化后的原子渗透集合$E' = E - e_j$。

NEG-NSAM方法基于原子渗透语义的相似性,提出了网络渗透图模型简化算法NEGSA(Network Exploitation Graph Model Simple Arithmetic)。NEGSA算法的主要思想是把网络系统中语义相似性的原子渗透进行聚合,减少原子渗透集合的基数,从而达到简化网络渗透图的目的。基于原子渗透语义相似性的聚合技术减少了网络系统中冗余的原子渗透,但是并没有对有效信息造成损失。详细的简化算法描述如下:

```
算法:网络渗透图模型简化算法
BEGIN PROC
  初始化时,设定 E' = E
  FOR EACH e_i ∈ E DO
    FOR EACH e_j ∈ E(j ≠ i) DO
      IF ((pre(e_i) = pre(e_j)) AND //满足语义相似性(1)
      (S_f ⊆ (S_p ∪ S_d) - post(e_i)) AND //满足语义相似性(2)
      (S_f ⊆ (S_p ∪ S_d) - post(e_j))) THEN
        E' = E' - e_j; //排除冗余的原子渗透
      END IF
    END FOR
  END FOR
END PROC
```

简化后的网络渗透图模型构造时间复杂度为$O(|EPL'| \cdot |E'|^2)$,其中EPL'为简化后的渗透路径集合,E'为简化后的原子渗透集合。随着网络规模的不断扩大,原子渗透语义相似性的概率就越大,其聚合的概率也就越大,简化后的$|EPL'| \ll |EPL|$,从而$O(|EPL'| \cdot |E'|^2) \ll O(|EPL| \cdot |E|^2)$。

3 应用实例

为了验证NEG-NSAM方法的可行性和有效性,本文构造了一个如图3所示的实验网络系统进行应用验证。图3中的网络系统由6个业务部门和1个信息中心组成,每个业务部门由20台工作站组成,信息中心由4台服务器组成。防火墙对外部网络设置了严格的访问控制策略,只允许外部访问者连接内部网络的WebServer、MailServer和FileServer服务器。各个实验室和管理部门之间都通过中心交换机设置了VLAN,互相不能进行访问。同时,WebServer、MailServer和FileServer服务器不能直接访问DBServer服务器。

假设实验网络系统的安全目标是保护DBServer,确保威胁主体无法获取其root权限。对网络系统进行参数获取,共发现存在150个脆弱性;在数据预处理阶段将网络参数进行格式转化,采用简化算法NEGSA后存在18个原子渗透;采用构造算法和绘制算法后生成的图形化的网络渗透图模型如图4所示。

图4所示的网络渗透图模型刻画了实验网络的安全态势,如外部威胁主体共存在40条渗透路径来获取DBServer的root权限。在图4的基础上还可以进行进一步的安全分析,如原子渗透集合$\{e_1, e_3, e_5\}$、$\{e_6, e_7, e_8\}$为实验网络系统的最小关键原子渗透集合。

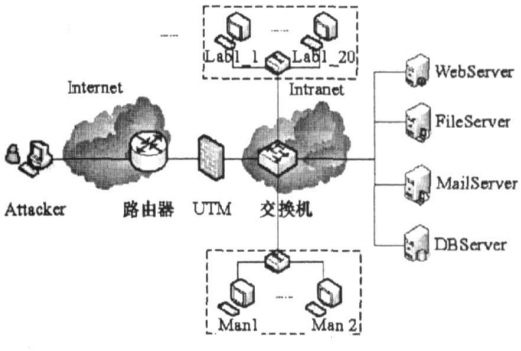


图 3 实验网络拓扑结构
Fig.3 Topology of experimental network

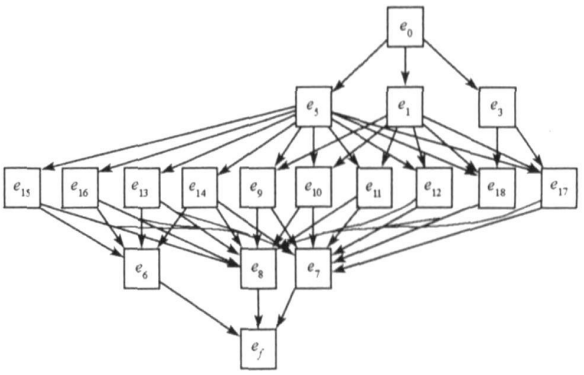


图 4 实验网络的网络渗透图模型
Fig.4 NEG of experimental network

4 结论和展望

对网络系统进行安全分析可以帮助认清安全现状, 进而采取有效和优化的安全措施。本文提出了一种基于图论的网络安全分析方法 NEG-NSAM, 在对网络系统参数进行抽象和对脆弱性进行关联分析的基础上, 构造网络渗透图模型, 准确刻画了威胁主体逐步渗透安全目标的动态过程。针对大规模网络环境, 提出了渗透图简化算法 NEGSA。最后, 运用 NEG-NSAM 方法对实验网络进行了分析。

针对研究过程中尚存在的一些缺陷, 今后将在如下方面进行进一步研究: (1) 提高网络系统参数抽象的完整性和准确性; (2) 网络脆弱性知识库的完善和扩充; (3) 有效的图形简化技术, 使渗透图模型适应更大规模的网络系统; (4) 更多具有实际意义的安全辅助决策技术。

参 考 文 献:

[1] Schneier B. Attack Trees[J]. Dr. Dobb's Journal, 1999, 24(12): 21- 29.
[2] Dacier M, Deswartes Y, Kaaniche M. Quantitive Assessment of Operational Security Models and Tools[R]. Technical Report Research Report 96493, LAAS, May 1996.
[3] Ortalo R, Deswarte Y, Kaaniche M. Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security[J]. IEEE Transactions on Software Engineering, 1999, 25(5): 633- 650.
[4] Swiler L P, Phillips C, Gaylor T. A Graph-based Network-vulnerability Analysis System[R]. Technical Report SAND97- 3010/1, Sandia National Laboratories, Albuquerque, New Mexico and Livermore, California, 1998.
[5] Jha S, Sheyner O, Wing J. Two Formal Analyses of Attack Graphs[C]// Proceedings: 15th IEEE Computer Security Foundations Workshop (CSFW' 15), Cape Breton, Nova Scotia, Canada, IEEE Computer Society, 2002: 49- 63.
[6] Ritchey R W, Ammann P. Using Model Checking to Analyze Network Vulnerabilities[C]// Proceedings: IEEE Computer Society Symposium on Security and Privacy (S&P 2000), Oakland, California, IEEE Computer Society, 2000: 156- 165.
[7] 汪立东. 一种量化的计算机系统和网络安全风险评估方法[D]. 哈尔滨: 哈尔滨工业大学, 2002.
[8] 胡华平, 等. 网络安全脆弱性分析与处置系统的研究与实现[J]. 国防科技大学学报, 2004, 26(1).
[9] 张永铮, 等. 基于特权提升的多维量化属性弱点分类法的研究[J]. 通信学报, 2004(7).
[10] 汪渊, 等. 基于图论的网络安全分析方法研究与应用[J]. 小型微型计算机系统, 2003(10).
[11] 董豆豆, 等. 基于故障树的系统安全风险实时监测方法[J]. 国防科技大学学报, 2006, 28(2).
[12] Li W. An Approach to Graph-based Modeling of Network Exploitations[D]. Department of Computer Science and Engineering, Mississippi State University, Mississippi State, Mississippi, 2005.
[13] 张义荣, 等. 计算机网络攻击效果评估技术研究[J]. 国防科技大学学报, 2002, 24(5).
[14] Ritchey R, Noel S. Representing TCP/IP Connectivity for Topological Analysis of Network Security[C]// Proc. of the 18th Annual Computer Security Applications Conference, 2002: 25- 31.
[15] Ammann P, Wijesekera D, Kaushik S. Scalable, Graph-based Network Vulnerability Analysis[C]// Proceedings: 9th ACM Conference on Computer and Communications Security (CCS' 02), Washington DC, 2002, ACM: 217- 224.
[16] Noel S, Jajodia S, O Berry B, et al. Efficient Minimum-cost Network Hardening Via Exploit Dependency Graphs[C]// Proceedings: 19th Annual Computer Security Applications Conference, Las Vegas, Nevada, 2003.