# 网络脆弱性分析方法的研究

倪评福[1],吴作顺[2]
(1. 西安通信学院,陕西 西安 710106;2. 中国电子设备系统工程研究所,北京 100141)

**摘 要**:网络脆弱性分析是网络安全分析和风险评估的重要组成部分。网络脆弱性分析方法的发展经历了从人工分析到自动分析的阶段,在自动化分析阶段,基于网络扫描的脆弱性分析发展得到了很大的进步。为了方便网络脆弱性的分析,提出了基于模型的分析方法,提出的各种基于模型的脆弱性分析方法从不同的角度入手,具有各自的优势。为了全面、准确地分析目标网络,必须考虑整个系统作为一个动态和分布式的特点,基于模型的分析方法可以分析整个网络,并可以利用强大的数学工具。

**关键词**:网络安全分析;脆弱性;Petri 网
**中图分类号**:TP393 **文献标识码**:A **文章编号**:1673-629X(2013)04-0126-05
doi:10.3969/j.issn.1673-629X.2013.04.031

# Research on Analysis Methods of Network Vulnerability

NI Ping-fu[1], WU Zuo-shun[2]
(1. Xi'an Communication Institute, Xi'an 710106, China;
2. China Electronic Installation Systems Engineering Company, Beijing 100141, China)

**Abstract**: Vulnerability analysis of network is an important part of network security analysis and risk assessment. Vulnerability analysis of network has experienced the stage from the manual to the automatic. In the automatic analysis stage, the scan-based vulnerability analysis methods have been well advanced. In order to be convenient for vulnerability analysis of network, the model-based analysis has been proposed. Many model-based vulnerability analysis methods start with different angles and have respective advantages. To make the result comprehensive and accurate, the target of analysis must be considered as a whole system with dynamic and distributed features. Model-based methods can analyse a whole network, and can use powerful mathematic tools.

**Key words**: network security analysis; vulnerability; Petri nets

## 0 引 言

随着计算机技术和网络技术的飞速发展,各领域使用计算机网络来协助工作越来越普遍,计算机网络在给人类社会带来便利的同时,也隐藏着越来越多的安全隐患。根据国家计算机网络应急技术处理协调中心(CNCERT/CC)近 4 年的网络安全工作报告,2009 年接收非扫描类网络事件为 21927 件,远远高于 2007 年的 4390 件和 2008 年的 5167 件。

经过互联网的发展,传统的网络安全事件得到了有效的治理,但是新型的网络安全事件仍然不断出现,网络安全呈现跨境化、趋利化、专业化等特点,网络安全仍然面临重大的挑战。

造成网络安全事件的根本原因是计算机网络的脆弱性。计算机系统是由一系列计算机系统实体的当前状态组成,根据安全策略定义将状态分为两种状态:已授权的状态和未授权的状态[1]。

脆弱状态是指从已授权的状态变换到未授权状态。脆弱性是指脆弱状态的特征,脆弱性可以是很多脆弱状态的特征[1]。

网络脆弱性分析通过对网络进行基于经验(知识)的分析或基于模型的分析等有效手段得出网络的脆弱性,然后评估网络安全,帮助管理员及时了解网络系统的安全状况,及时发现并修补漏洞,避免网络攻击。文中将网络脆弱性分析方法进行归纳分类,并指出各自的优缺点,对今后研究有借鉴作用。

## 1 网络脆弱性分析方法分类

网络脆弱性分析方法按照分析之前是否进行建模分为基于经验(知识)的脆弱性分析方法和基于模型的脆弱性分析方法,基于经验(知识)的分析方法又分为基于规则的分析方法和基于案例的分析方法。基于模型的分析方法又可以分为基于单一关系模型和基于

**收稿日期**:2012-05-31;**修回日期**:2012-09-04
**基金项目**:国防 973 项目(6131180401)
**作者简介**:倪评福(1988-),男,硕士研究生,主研方向为网络安全。

多关系模型。

## 2　基于规则的分析方法

从已知的脆弱性中抽取特征,并归纳为规则表达式,将目标系统与已有的规则一一匹配,通过这种方法来寻找目标系统中存在的脆弱性。

基于规则的分析方法应用最广的就是网络安全扫描工具。网络安全扫描又根据运行的位置不同,可以分为两类:基于主机的扫描分析和基于网络的扫描分析。

### 2.1　基于主机的扫描分析

基于主机的脆弱性扫描,就是在目标系统上安装漏洞扫描器,对本地文件内容、系统的设置以及其他同安全规则抵触的对象进行扫描分析。

基于主机的漏洞扫描体系通常是一个基于主机的 Server 三层体系结构:漏洞扫描控制台、漏洞扫描管理器和漏洞扫描代理。

在每个目标系统都安装漏洞扫描器代理,向漏洞管理器进行注册,漏洞控制器通过漏洞管理器下发扫描指令和回收扫描结果,用户通过漏洞控制器下发扫描指令和查看扫描结果。

基于主机的扫描分析具有的优势:

(1)更加准确地发现系统漏洞;

(2)能够访问目标系统的所有文件与进程,能够发现更多的脆弱性;

(3)网络性能影响小。

同时具有的劣势是:

(1)效率低;

(2)扫描远程渗透式弱点能力弱。

### 2.2　基于网络的扫描分析

基于网络的脆弱性扫描就是向目标发送特殊制作的数据包,通过查看目标的反应以及分析目标应答的形式和内容,判断目标是否存在已知的脆弱点[2]。

基于网络的扫描分析具有的优势:通用性强、安装方便、效率高。

同时具有的劣势:

(1)不能检查不恰当的本地安全策略;

(2)影响网络的性能。

## 3　基于案例的分析方法

基于案例的分析方法就是从分析以往的案例抽取经验(知识)用于分析今后的案例。现在应用比较广的是基于案例推理技术(Case-based reasoning,简称 CBR):将新的案例与案例库中的特征值进行对比,找到与新案例相似的旧案例,从旧案例解决方案中推理出新案例的解决方法[3]。

基于案例推理的过程图如图 1 所示。当遇到目标问题时,分析提取案例的特征,在案例数据库中查找相同特征的案例,如果找出相应的案例,利用此案例的解决方案来解决新的案例问题,如果对解决方案不满意,则对解决方案进行修改并将最终的解决方案作为一个新的案例保存在案例数据库中,如果检索不到类似的案例,则创建一个新案例,并通过案例学习增加解决方法并保存在案例库中。

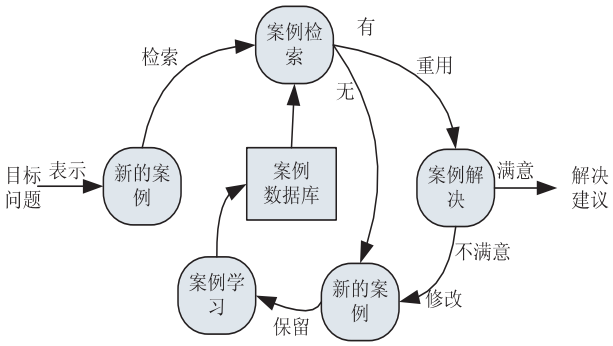



图 1　基于案例推理的过程图

基于案例推理的优势:

(1)知识的获取比规则的获取更加简单;

(2)基于案例推理能够实现自我学习的功能。

同时具有的劣势:无法对单个漏洞进行描述。

## 4　基于模型的分析方法

基于图论的分析方法就是根据网络各节点之间的关系建立模型。

### 4.1　基于单一关系模型的分析方法

#### 4.1.1　基于漏洞依赖关系的分析方法

漏洞依赖关系图,是将漏洞用节点表示,漏洞之间的依赖关系用边表示,将复杂的计算机网络简化成漏洞依赖关系图。在漏洞依赖关系图中,找出可达的最终攻击状态,逆向分析找出可能的攻击路径,去掉冗余的节点和边,利用各漏洞的难易程度,选择出一条最容易受到攻击的攻击路径[4]。

基于漏洞依赖关系图,具有的优势:构建形成漏洞依赖图简单方便。同时具有的劣势:没有中间状态,不方便动态分析。

#### 4.1.2　基于状态转移图的分析方法

状态转移图分析最早是由 Kemmerer 提出[5],状态转移图是指入侵者的状态改变图,将入侵者的状态作为节点,改变入侵者状态的漏洞作为边,将计算机网络简化成入侵者状态变化图。由于入侵者的状态是有限的,也可以人为设置入侵者状态的数量,从而可以有效减小状态转移图的复杂度。

#### 4.1.3　基于攻击图的分析方法

攻击图技术根据网络状态和脆弱性信息,分析出

攻击者对网络漏洞的利用序列,并将这些序列进行优化形成一张有向图,即攻击图[6~8]。

攻击图用四元组 $G=(S,R,S_0,S_S)$ 表示。其中,$S$ 是状态节点的集合;$R\subseteq S\times S$,表示变迁关系;$S_0\subseteq S$ 是初始状态的集合;$S_S$ 是目标状态(即攻击成功状态)的集合。

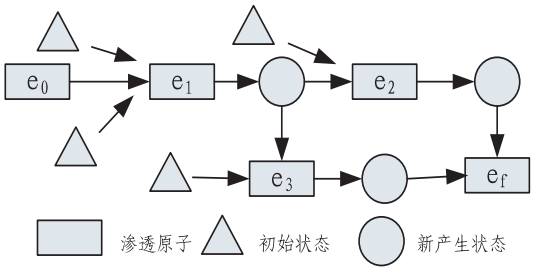
对于一个目标状态 $S_N\in S$,如果从初始状态 $S_0$ 开始,存在一组状态序列 $S_1,S_2,\cdots,S_{N-1}$,使得 $(S_i,S_{i+1})\in R,0\leqslant i\leqslant n-1$,则称状态序列 $S_0,S_1,S_2,\cdots,S_N$ 是一条攻击路径。

把各个节点初始化为(S,D,V)。其中 S 和 D 代表两个可以互通的主机,V 代表主机 D 上的漏洞。而边可以用二元组(H,C)表示,其中 H 代表主机,C 代表主机满足的攻击条件,也只有 C 满足了某个攻击条件时,初始节点才能沿该边到达中间节点,如此一步一步最终达到目标节点。

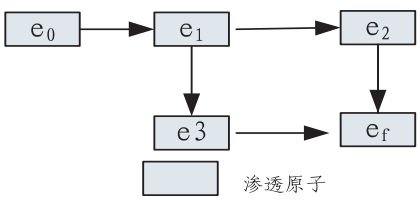
基于攻击图具有的优势:从攻击者的角度来分析问题。

#### 4.1.4 基于渗透图的分析方法

文献[9]提出了网络渗透图模型的概念,网络渗透图模型描述了威胁主体到达目标状态所有可能的渗透路径,其节点表示网络中的原子渗透,边表示渗透行为造成网络状态的变化。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 2(a)表示含有网络状态信息的图形化的网络渗透图模型;图 2(b)表示标准的图形化的网络渗透图模型[9]。




(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 2 图形化的网络渗透图模型

基于渗透图模型具有的优势:可以描述攻击者多阶段入侵的行为。

#### 4.1.5 基于贝叶斯的分析方法

贝叶斯网络是一个有向无环图,图中的节点代表随机变量,弧代表影响概率[10],弧的方向代表了两个节点之间的因果影响关系。一个简单的贝叶斯网络的示例如图 3 所示。在给定贝叶斯网络的节点子集的情况下(如表 1 所示),可以计算另一个节点自己的条件概率分布(如表 2 所示)。

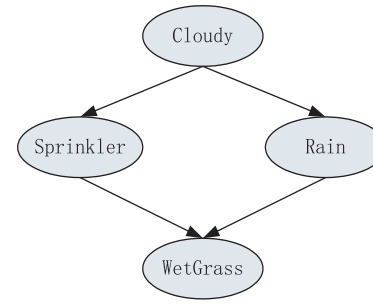



图 3 四个变量的贝叶斯网络

表 1 条件概率表(1)

| W | P(S=F) | P(S=T) | W | P(R=F) | P(R=T) |
|---|---|---|---|---|---|
| F | 0.5 | 0.5 | F | 0.8 | 0.2 |
| T | 0.9 | 0.1 | T | 0.2 | 0.8 |

表 2 条件概率表(2)

| S | R | P(W=F) | P(W=T) |
|---|---|---|---|
| F | F | 1.0 | 0.0 |
| T | F | 0.1 | 0.9 |
| F | T | 0.1 | 0.9 |
| T | T | 0.01 | 0.99 |

基于贝叶斯网络的分析方法具有的优势:适用于对不确定性知识的表达和推理。同时具有的劣势:网络复杂时,计算量很大。

#### 4.1.6 基于 Petri 网

在 Petri 网中,用库所 W 表示系统的状态,用变迁表示改变状态的事件,将计算机网络用库所和库所变迁表示。在 Petri 网图形表示中“|”代表库所,“0”代表变迁,“→”表示有向弧,图中的实心圆点代表令牌[11,12]。

基于 Petri 网模型具有的优势:

(1)具有优良的数学性质,和网络系统中常见的同步、冲突、并发、资源共享等现象相似,可以用 Petri 网模型来仿真相应的现象;

(2)Petri 网内部拥有丰富的分析工具,可以直接在此基础上直接进行分析。同时具有的劣势:模型比较复杂。

### 4.2 基于多关系模型的分析阶段

#### 4.2.1 基于贝叶斯网络的信息安全风险概率计算模型

文献[13]定义基于贝叶斯网络的信息安全风险概率计算模型 PEG-BN={PEG, $P$}:PEG 为渗透图,反应了原子风险渗透之间的因果关系。$P=\{P(ae_i\mid Pa(ae_i),ae_i\in AE)\}$ 是 PEG 中原子风险渗透发生的条件概率的集合[13]。一个简单的信息安全

风险概率计算模型如图 4 所示[14]。

建立 PEG-BN 模型网络结构算法:

(1)在 PEG-BN 模型中建立一个二态节点,并命名为 $ae_0$;

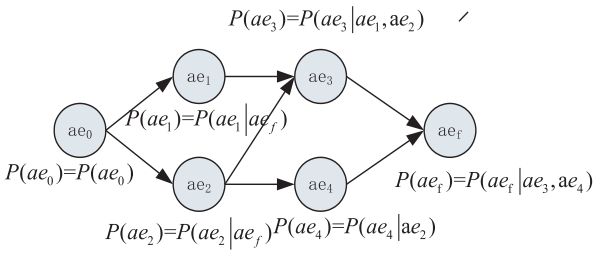



图 4　信息安全风险概率计算模型

(2)对 $ae_0$,寻找其所有直接后续的原子风险渗透 $ae_i$,$ae_i$ 为此时 PEG-BN 模型的叶节点;

(3)对图 4 中的所有叶节点 $ae_i$,寻找其所有直接后续的原子风险渗透节点 $ae_j$,$ae_j$ 为此时 PEG-BN 模型的叶节点;

(4)重复(3)的做法,直至遍历完 PEG 模型中的所有原子风险渗透。

基于贝叶斯网络的信息安全风险概率计算模型具有的优势:

(1)模型构建方便,同时利用贝叶斯学习,方便对网络进行更新;

(2)基于贝叶斯网络的信息安全风险概率符合系统安全风险的实际情况;

(3)基于贝叶斯网络模型有利于风险预测和实时评估。

同时具有的劣势是:

(1)各个脆弱性被利用的概率是人为来设置,缺乏客观性;

(2)随着网络的扩大,计算量成指数增长,不利于大规模网络仿真。

#### 4.2.2　基于可靠性理论的分布式系统脆弱性模型

分布式系统是建立在网络之上的软件系统。分布式系统的特点是计算分布化、用户分布化、资源分布化和管理分布化,大型的分布式系统通常包含多个节点、平台和应用,并通过多种模式连接[15]。

文献[16]分布式系统的脆弱性模型选取的因素:

(1) $H$:分布式系统的主机集合。分布式系统中的任何一台主机 $h \in H$,都用一个五元组(id,usr,svcs,sw,vuls)来表示,分别表示(主机的唯一标识符,主机设置的用户类型,主机上运行的应用服务,主机上安装的软件,主机上存在的漏洞);

(2) $I$:入侵模型,$plvl(h) \rightarrow \{\text{none},\text{user},\text{root}\}$;

(3) $R$:主机间的连接关系,$R \subseteq \text{Host}\times\text{Host}\times\text{Port}$;

(4) $T$:主机间的信任关系,$\text{RshTrust} \subseteq \text{Host}\times\text{Host}$;

(5)IDS:入侵检测系统模型,$\text{ids} \subseteq \text{Host}\times\text{Host}\times\text{Action} \rightarrow \{d,s,b\}$ 分别表示 Action{可检测,隐秘,既有可检测部分又有隐秘部分};

(6) $S$:分布式系统的状态集合,该集合中的任一状态都表示为 $s=(\text{sub},\text{obj},\text{env})\rightarrow$(主体条件,客观条件,环境条件);

(7) $A$:行为集合。$a=(\text{ID},\text{Name},\text{VulID},s_s,s_d,\lambda)$ 表示(唯一编号,名称,漏洞编号,源状态,目标状态,难易程度的代价参数);

(8) $G$:系统的安全属性集合,即分布式系统所要达到的安全防护目标。

基于分布式系统脆弱性模型具有的优势:

(1)分布式系统脆弱性模型采用系统状态作为节点更适合仿真计算机网络,系统的脆弱性不仅仅来源于攻击,更来源于系统自身配置;

(2)与以网络漏洞为节点的攻击图相比,分布式系统脆弱性模型更能节省状态空间。

#### 4.2.3　基于脆弱性关联模型的网络威胁分析

文献[17]基于脆弱性关联模型的建模:

(1)为网络的每个节点创建节点对象,节点对象是每一个网络节点信息的封装体,它是一个三元组 $\langle A,M,R\rangle$,对应节点对象的属性集,对象中的封装方法,节点对象之间的关联关系;

(2)属性集 $A=\langle \text{sta\_att},\text{dyn\_att}\rangle$ 描述节点对象的状态信息;

(3)方法 $M$ 描述了攻击者对节点对象的攻击行为,它是一系列函数的集合;

(4)关联关系 $R$ 为一个三元组 $R=\langle \text{PR},\text{AR},\text{TR}\rangle$,PR 为物理连接关系,AR 为访问关系,TR 为信任关系。

在建立的网络脆弱性关联模型上采用 Dijkstra 算法计算任意一个节点的威胁度。具体算法参考文献[17,18]。

## 5　分析方法存在的问题

(1)在复杂网络环境下对新的脆弱性特征抽取形成规则表达越来越复杂,在网络脆弱性知识库越来越大的情况下,规则匹配的复杂性不断提高,同时网络数据流量越来越大,导致规则匹配成为大量数据包脆弱性扫描分析的瓶颈。

(2)目前的脆弱性分析缺乏对网络自身配置情况和人为管理等方面的研究。

(3)目前基于攻击图和状态图的分析方法存在着状态空间爆炸问题,状态空间爆炸问题是大规模网络脆弱性分析的瓶颈。

(4)缺乏统一的脆弱性评估量化指标,对各种量化指标得出的结果难以进行比较。

## 6 结束语

各种网络脆弱性分析方法从不同的角度入手,在解决特定问题时各有优点,例如:基于扫描分析更适于查找已知漏洞;攻击图更适于系统安全性分析、入侵行为分析。在分析实际网络安全时,应根据实际情况和安全要求选择合适的模型或者对现有模型进行改进,将实际网络中与安全有关的局部信息一步一步地加入模型,使得模型具有更强的解决实际问题的能力。

脆弱性评估方法的发展经历了人工分析到自动分析的阶段,现在正在由局部分析向整体分析发展,由基于扫描分析方法向基于模型的分析方法发展,由静态分析向动态分析发展,由单机分析向分布式分析发展。

**参考文献:**


[1] Bishop M, Bailey D. A critical analysis of vulnerability taxonomies[R]. Davis: University of California at Davis, 1996.

[2] 刘海燕,杨洪路,王 崛. 一个基于网络的脆弱性扫描系统[J]. 计算机应用,2003,23(7):98-99.

[3] 林 闯,汪 洋,李泉林. 网络安全的随机模型方法与评价技术[J]. 计算机学报,2005,28(12):1943-1956.

[4] Noel S, Jacobs S, Jacobs M. Efficient Minimum-cost Network Hardening via Exploit Dependency Graphs[C]//Proc of the 19th Annual Computer Security Applications Conference. Las Vegas, Nevada: [s. n.], 2003: 86-95.

[5] Ilgun K. USTAT: A real-time intrusion detection system for UNIX[C]//Proc of IEEE Symposium on Research in Security and Privacy. Oakland, CA: [s. n.], 1993.

[6] Swiler L P, Phillips C, Gaylor T. A graph-based network-vulnerability analysis system[R]. Sandia: Sandia National Laboratories, 1997.

[7] Li W. An Approach to Graph-based Modeling of Network Exploitations[D]. Mississippi State: Mississippi State University, 2005.

[8] Noel S, Jajodia S, Berry B, et al. Efficient Minimum-cost Network Hardening via Exploit Dependency Graphs[C]//Proceedings of the 19th Annual Computer Security Applications Conference. Las Vegas, Nevada: [s. n.], 2003: 1-10.

[9] 张维明,毛捍东,陈 锋. 一种基于图论的网络安全分析方法研究[J]. 国防科技大学学报,2008,30(2):97-101.

[10] Liu Yu, Man Hong. Network Vulnerability Assessment Using Bayesian Networks[C]//The International Society for Optical Engineering. San Diego, CA: SPIE Press, 2005: 61-71.

[11] Girault C, Valk R. Petri Nets for Systems Engineering: A Guide to Modeling, Verification, and Application[M]. Berlin Heidelberg: Springer-Verlag, 2003: 1-14.

[12] 林 闯. 随机 Petri 网和网络系统性能评价[M]. 第 2 版. 北京:清华大学出版社,2000:5-21.

[13] 王桢珍,姜 欣. 信息安全风险概率计算的贝叶斯网络模型[J]. 电子学报,2010(BO2):18-22.

[14] 张金槐,刘 琦,冯 静. Bayes 试验分析方法[M]. 长沙:国防科大出版社,2007.

[15] 毛捍东. 基于逻辑渗透图模型的网络安全风险评估方法研究[D]. 长沙:国防科学技术大学,2008.

[16] 冯萍慧,连一峰,戴英侠,等. 基于可靠性理论的分布式系统脆弱性模型[J]. 软件学报,2006(7):1633-1640.

[17] 王纯子,黄光球. 基于脆弱性关联模型的网络威胁分析[J]. 计算机应用,2010,30(11):3047-3050.

[18] 邢栩嘉,林 闯,蒋屹新. 计算机系统脆弱性评估研究[J]. 计算机学报,2004,27(1):1-11.


(上接第 106 页)

还处于测试阶段,对于采样时间戳的控制等功能的完善还需要进一步推进。

**参考文献:**


[1] Chen Lei, Jian Wei, Li Yanbo, et al. Research of Performance Monitoring for Spatial Information System[C]//2010 International Conference on Future Information Technology and Management Engineering. [s. l.]: [s. n.], 2010.

[2] Merkel R. Secure Shell[EB/OL]. 2005[2009-09-12]. http://en. wikipedia. org/wiki/Secure_Shell.

[3] 余永洪. 用 SSH 技术远程管理 Linux 服务器[J]. 计算机与现代化,2007(7):96-98.

[4] 马昕炜. Linux 系统管理员手册[M]. 北京:北京希望电子出版社,2005.

[5] 陈永建,朱 娟,黎桂林. 基于 WMI 的实时监控系统设计与实现[J]. 微计算机信息,2005(21):47-49.

[6] Ivorson T. Windows Management Instrumentation[EB/OL]. 2004[2012-09-04]. http://en. wikipedia. org/wiki/Windows_Management_Instrumentation.

[7] Polichat M. WMI 技术指南[M]. 北京:机械工业出版社,2003:5-40.

[8] 卜春芬. C#后台处理与多线程技术的应用[J]. 昆明学院学报,2010(3):88-91.

[9] 陈少强. VC++中基于 MFC 的多线程应用程序设计[J]. 三明高等专科学校学报,2002(2):49-55.

[10] 多线程[EB/OL]. 2012-09-01. http://baike. baidu. com/view/65706. htm.

[11] Nagel C, Evjen B, Glynn J. C#高级编程[M]. 李敏波译. 第 4 版. 北京:清华大学出版社,2006:153-163.

[12] Dmerrill. Linux[EB/OL]. 2001[2012-09-08]. http://en. wikipedia. org/wiki/Linux.