一种基于攻击图的漏洞风险评估方法

张 玺，黄曙光，夏 阳，宋舜宏
（电子工程学院 网络系，合肥 230037）

摘 要：传统的安全漏洞评估方法只是孤立地对单个漏洞进行评估，评估结果不能反映出漏洞对整个网络的影响程度。针对这个问题，提出了一种新的漏洞风险评估方法。该方法根据攻击图中漏洞间的依赖关系与漏洞的 CVSS 评分，首先计算出漏洞被利用的可能性与被利用后对整个网络的危害程度，并在此基础上计算出漏洞具有的风险值。由该方法计算出的漏洞风险能够准确地反映出漏洞对整个网络的影响程度，并通过实验证明了该方法的准确性与有效性。

关键词：安全漏洞；攻击图；渗透
中图分类号：TP393 **文献标志码**：A **文章编号**：1001-3695(2010)01-0278-03
doi:10.3969/j.issn.1001-3695.2010.01.082

Attack graph-based method for vulnerability risk evaluation

ZHANG Xi, HUANG Shu-guang, XIA Yang, SONG Shun-hong
(*Dept. of Network, Electronic Engineering Institute, Hefei* 230037, *China*)

Abstract: The conventional methods for vulnerability risk evaluation just concentrate on individual vulnerability, which can't reveal impact on the whole network. For this problem, this paper put forward a new method for vulnerability risk evaluation. Based on casual relationship between vulnerabilities in attack graph and CVSS score of vulnerabilities, this method first computed the probabilities of exploits and the impact on the whole network after exploits, and then computed vulnerability risk. The vulnerability risk can exactly reveal its impact on the whole network. Experiment validates its veracity and validity.

Key words: vulnerability; attack-graph; exploit

随着网络的深入和快速发展，网络安全问题日益突出，对网络安全状况进行定量分析显得尤为重要。安全漏洞[1]是指系统软件或硬件存在着某种形式的脆弱性，这种脆弱性存在的直接后果就是允许非法用户在未经授权就能获取或提高访问权限。安全漏洞的大量存在是安全问题的总体形势趋于严峻的重要原因之一[2]，因此对漏洞进行准确、合理的风险评估，对于网络安全管理来说有着非常重要的意义。已有的漏洞风险评估大部分采用专家评判的方法，根据漏洞的严重程度、影响和风险等因素，对漏洞进行定性或定量的划分[3,4]。这种评估方式主观性较强，而且主要针对单个漏洞，没有考虑漏洞所处的网络环境，因而不能真实地反映出漏洞具有的风险。

攻击图描述了攻击者在网络系统中利用系统脆弱性进行渗透、逐步提升权限的过程，体现了漏洞间的相互利用关系[5~7]。在攻击图的基础上，提出了一种漏洞风险评估方法。该方法利用漏洞的 CVSS 评分[4]对漏洞本身的固有属性进行量化，根据攻击图中漏洞间的关联关系，能够客观、准确地计算出漏洞对整个网络具有的风险。根据漏洞的风险等级，安全人员可以很清楚地识别安全隐患，集中精力消除最具危害性的漏洞，极大提高了网络安全管理的效率。

1 攻击图模型

从网络安全事件的统计结果可以看出，多数的网络攻击都利用了已知的网络弱点，并且攻击者经常利用不同主机上的弱点进行跳跃式的攻击。包含攻击者可能采取的网络攻击行为以及攻击行为之间依赖关系的图称为网络攻击图[8]。

攻击图是一种有向图，根据有向图中点和边的具体意义，攻击图可以分为以下两类[9]：

a)状态列举图。攻击图中的每个节点代表整个系统一个可能的攻击状态，攻击状态是由系统当前的一组安全属性组成的，这些属性通常包括相关的主机名、攻击者在相关主机上获取的权限、相关主机存在的漏洞、开放的服务等。攻击图中的每条有向边代表攻击者利用一个单一的脆弱性进行渗透从而引起的状态改变。

b)渗透依赖图。与状态列举表示法不同，该攻击图中的每个节点代表系统的一个安全属性。有向弧线代表一个渗透，由渗透的前提条件指向渗透结果。

这两种攻击图的主要不同之处在于节点代表的含义不同。状态列举图中的每一个节点代表了整个网络的一个安全状态，而渗透依赖图中的每一个节点只代表了网络的安全属性。状态列举图类似于一个状态转移图，它描述了攻击者所有可能的渗透序列，但没有描述安全属性之间的依赖关系。而在渗透依赖图中，安全属性之间的依赖关系用有向边明确表示出来。本文采用渗透依赖图表示每个安全属性间的依赖关系。

渗透依赖图是一个有向图 $G(E\cup C, R_r\cup R_i)$[9]。其中：E 为渗透节点集合，C 为条件节点集合。$R_r\subseteq C\times E$，$R_i\subseteq E\times C$。

收稿日期：2009-03-02；**修回日期**：2009-06-17

作者简介：张玺(1982-)，男，河北辛集人，硕士研究生，主要研究方向为网络安全(zhangxi8211@163.com)；黄曙光(1964-)，男，安徽合肥人，教授，博导，主要研究方向为信息安全；夏阳(1977-)，男，安徽淮南人，讲师，博士，主要研究方向为网络安全；宋舜宏(1971-)，男，安徽安庆人，博士研究生，主要研究方向为网络安全.

$E \cup C$ 为所有节点集合,$R_r \cup R_i$ 为有向边集合。

从定义可以看出,渗透依赖图中的有向边存在两种类型。第一种有向边 R_r 由一个条件节点指向一个渗透节点。一个渗透的所有前提条件都满足之后,该渗透才能完成,因此指向同一个渗透节点的边之间为“与”关系。第二种有向边 R_i 由一个渗透节点指向一个条件节点,表示渗透所造成的结果。由于多个渗透可以造成同一种结果,指向同一个条件节点的边之间为“或”关系。

2　基于攻击图的漏洞风险评估

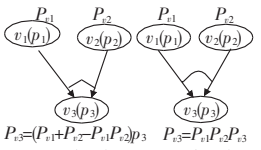
从攻击图中可以看出,一个漏洞被利用后导致了其他的漏洞被利用,因此一个漏洞不仅对所在的主机造成了危害,对网络中其他主机也产生了危害。这两种危害之和反映了漏洞对整个网络的危害。一个漏洞对整个网络的危害和它被攻击者成功利用的概率共同决定了一个漏洞的总风险。

2.1　漏洞的成功利用概率

定义 1　漏洞的固有概率 p 表示在所有条件满足的情况下,漏洞被成功利用的概率。这个概率取决于漏洞利用的难易程度。

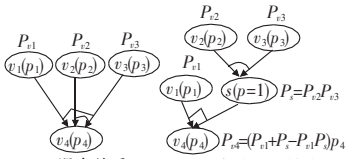
定义 2　漏洞的累积概率 P 表示攻击者成功利用网络中一个漏洞的概率。用累积概率表示漏洞被成功利用的概率,它与漏洞的固有概率和攻击路径有关。

攻击图中包含了权限、漏洞、访问控制关系等信息。为了便于分析,需要对攻击图进行简化。简化后的攻击图只剩下代表漏洞的节点,漏洞间的利用关系保持不变。这样得到的简化图是一张漏洞利用关系图。漏洞利用关系图表示了漏洞利用的先后关系与逻辑关系。先后关系通过有向边表示出来。逻辑关系的存在是由于攻击图中节点间存在着“或”关系和“与”关系,漏洞利用关系图中的节点之间也存在着两种关系。图 1(a)显示的是一种“或”关系,表示可以通过漏洞 v_1 利用漏洞 v_3,也可以通过漏洞 v_2 利用漏洞 v_3,这类似于随机事件中的“和事件”。漏洞 v_3 的累积概率计算方法如图 1(a)所示。图 1(b)显示的是一种“与”关系,表示利用漏洞 v_3 需要首先利用漏洞 v_1 和 v_2,这类似于随机事件中的“积事件”。漏洞 v_3 的累积概率计算方法如图 1(b)所示。漏洞利用关系图中的有向边之间还可能存在一种混合关系,如图 2(a)所示;可以通过添加一个“哑”节点把混合关系转换为“或”关系和“与”关系[9],如图 2(b)所示。



(a) “或”关系　(b) “与”关系

图 1　有向边之间的两种关系



(a) 混合关系　(b) 混合关系的转换

图 2　混合关系及其转换

根据图 1 计算“或”关系和“与”关系的方法,从初始节点开始,采用广度优先的方式,可以逐步计算出每个漏洞被成功利用的概率。

2.2　漏洞的危害程度

定义 3　漏洞的固有危害程度 ϕ 表示一个漏洞对一台主机造成的危害程度。

网络中的每台主机根据其扮演的角色不同,具有不同的价值量[10]。主机的价值量取决于主机的类型、主机中数据的重要性等许多因素。例如,一台数据库服务器具有的价值量要比一般用户的主机具有的价值量高,因为一旦数据库服务器被攻击者控制,许多重要信息将被泄露、修改或删除。用 ω 表示一台主机的价值量,一个漏洞对主机造成的损失则为 $\phi \cdot \omega$。

定义 4　漏洞的全局损失 W 表示一个漏洞对整个网络造成的总损失。一个漏洞的全局损失分为两部分。一部分是漏洞自身造成的损失;另一部分是该漏洞直接导致的其他漏洞造成的损失。

为了计算漏洞造成的全局损失,把漏洞利用关系图中节点的权值重新表示为漏洞造成的固有危害程度 ϕ(开始节点的权值为 0),有向边的权值仍表示漏洞 v 的固有概率。由于多个漏洞可能位于同一个主机上,也可能位于不同的主机上,计算一个漏洞造成的全局损失需要考虑漏洞在主机上的分布情况。图 3 给出了四种最基本的漏洞分布情况,并给出了每种情况下漏洞全局损失的计算方法。其他复杂的漏洞分布可以先分解为这四种最基本的情况,然后再计算漏洞的全局损失。

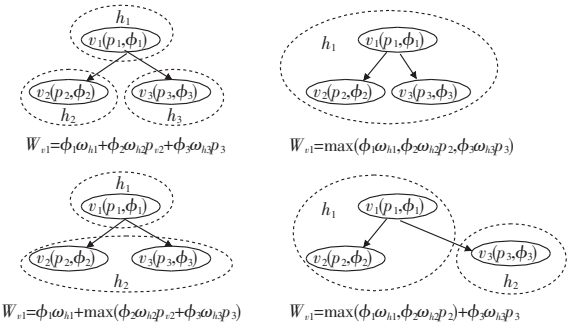


图 3　四种漏洞分布情况

定义 5　漏洞的全局危害程度 Φ 等于漏洞造成的全局损失与网络的最大损失量的比值。网络的最大损失量等于所有主机的价值量之和。

2.3　漏洞的风险

定义 6　一个漏洞的风险 R 等于漏洞被利用的概率 P(即累积概率)与全局危害程度 Φ 之积,即 $R = P \times \Phi$。

计算漏洞的风险需要三个参数:漏洞的固有概率 p、漏洞的固有危害 ϕ、每个主机的价值量。本文中前两个参数的取值从漏洞的 CVSS 评分中获得,每个主机的价值量由人为指定。

CVSS 评分包括基本分、临时分和环境分。其中,基本分反映了漏洞固有的本质特性,是不随时间和环境变化的。基本分又包括利用分和影响分。利用分从访问方式、访问复杂度和认证三个方面来衡量漏洞被利用的难易程度,其满分为 10,分数越高说明越容易被利用。用利用分除以满分 10 表示漏洞的固有概率。影响分从机密性影响、完整性影响和可用性影响三个方面来衡量一个漏洞的危害性,其满分为 10,分数越高说明造成的危害越大。用影响分除以满分 10 表示漏洞的固有危害程度。依据漏洞利用关系图和漏洞的 CVSS 评分计算漏洞风险的方法如图 4 所示。

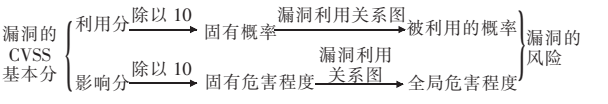


图 4　漏洞风险的计算方法

3　实验

本文中的实验网络(图 5)类似于文献[11]中的实验网络。网络中有三台主机,H1 为一般用户的主机,H2 上运行 Web 和 FTP 服务,H3 是一台数据库服务器。防火墙只允许

Internet访问内部网络 H2 上的 Web 服务和一般用户访问 Internet。攻击者(H0)位于 Internet 中,其攻击目标是获得数据库服务器的管理员权限,从中获取敏感数据。网络中存在的漏洞如表 1 所示。根据文献[6]中提出的攻击图生成方法,生成该实验网络对应的攻击图,如图 6 所示。通过对图 6 进行简化,得到漏洞利用关系图,如图 7 所示。

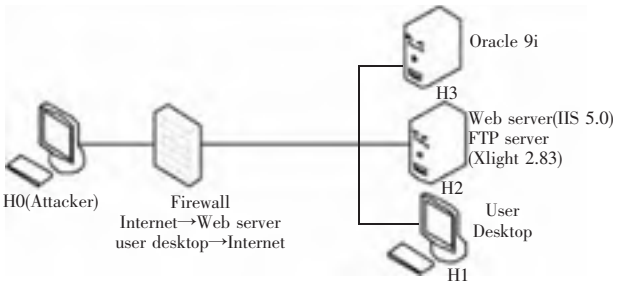


图 5　实验网络的拓扑结构

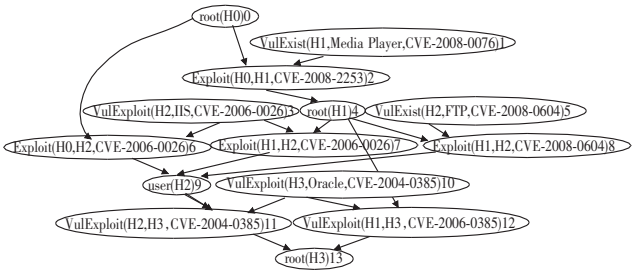


图 6　实验网络对应的攻击图

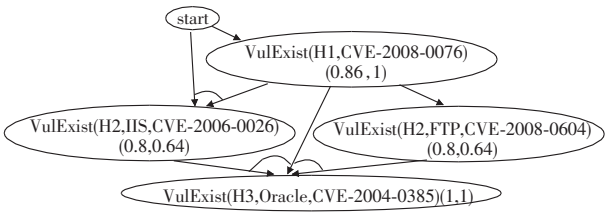


图 7　漏洞利用关系图

表 1　实验网络中漏洞的详细情况

漏洞所在主机	漏洞 CVE 编号	利用分/影响分	漏洞描述
H1	CVE-2008-0076	8.6/10	Internet Explorer 浏览器存在“HTML Rendering Memory Corruption”漏洞。当用户访问一个恶意网站时,远程攻击者可以通过恶意构造的网页在用户主机上执行任意指令
H2	CVE-2006-0026	8/6.4	MicroSoft IIS 存在缓冲区溢出漏洞。远程攻击者通过向 ASP 页面传送恶意输入导致缓冲区溢出,使得攻击者可以执行任意指令
H2	CVE-2008-0604	8.6/6.4	XLight FTP 服务中的 LDAP 认证方式存在空密码漏洞,当未指定 LDAP 服务器时,使得远程攻击者使用空密码便可登录
H3	CVE-2004-0385	10/10	Oracle 9i 存在堆溢出漏洞。远程攻击者通过构造一个长的 HTTP 请求,可导致 Oracle 9i 的 Web 服务缓冲区溢出,使得攻击者可以执行任意指令

根据漏洞利用关系图和漏洞的 CVSS 评分计算出每个漏洞的风险,计算结果如表 2 所示。计算中指定内部网络中所有主机的价值量之和为 1,一般用户占 10%,Web/FTP 服务器占 40%,数据库服务器占 50%。

表 2　漏洞风险评估结果

漏洞 CVE 编号	漏洞所在主机	主机的价值量	漏洞被利用的概率	漏洞的全局危害程度/%	漏洞的风险/%
CVE-2008-0076	H1	0.1	0.86	82.02	70.54
CVE-2006-0026	H2	0.4	0.8	75.60	60.48
CVE-2008-0604	H2	0.4	0.74	75.60	55.94
CVE-2004-0385	H3	0.5	0.99	50.00	49.50

从表 2 中可以得知,一般用户主机上的漏洞具有的危害程度最高,这是因为该漏洞容易被攻击者利用,而且被利用后能够导致网络中所有主机处于危险境地。Web/FTP 服务器上两个漏洞的全局危害程度相同,但由于被利用的概率不同,具有的风险也不同。数据库服务器上的漏洞虽然被利用的可能性最高,但是该漏洞只导致数据库遭受损失,因此具有的风险相对较低。以上分析表明,本文中提出的评估方法能够准确反映出漏洞具有的风险。

4　结束语

本文提出的漏洞风险评估方法不仅考虑了漏洞本身固有的属性,而且考虑了漏洞间的关联关系。漏洞本身固有的属性采用广泛公认的 CVSS 评分作为量化标准,具有可靠的计算依据。漏洞间的关联关系从攻击图中获得,能够全面地反映出漏洞间的各种关系。实验表明,该方法能够准确地评估漏洞具有的风险,评估结果与实际情况保持一致。网络管理人员根据漏洞不同的风险等级,可以着力解决最具危害性的漏洞,极大地提高了网络管理的效率。

参考文献:

[1] GB 征求意见稿,信息安全风险评估指南[S]. 北京:国务院信息化工作办公室,2005.

[2] 张永铮,方滨兴,迟悦. 计算机弱点数据库综述与评价[J]. 计算机科学,2006,33(8):19-21.

[3] 张涛,胡铭曾,李东,等. 一种量化的软件弱点评估方法[J]. 计算机工程与应用,2005,41(27):7-9.

[4] MELL P, SCARFONE K, ROMANOSKY S. A complete guide to the common vulnerability scoring system version 2.0[EB/OL]. [2008]. http://www.first.org/cvss/.

[5] OU Xin-ming, BOYER W F, McQUEEN M A. A scalable approach to attack graph generation[C]//Proc of the 13th ACM Conference on Computer and Communications Security. 2006:336-345.

[6] 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.

[7] SHEYNER O, HAINES J, JHA S, *et al*. Automated generation and analysis of attack graphs[C]//Proc of IEEE Symposium on Security and Privacy. Oakland, California: IEEE Press, 2002:254-265.

[8] 孙亮,李东,张涛. 网络攻击图的自动生成[J]. 计算机应用研究,2006,23(3):119-122.

[9] WANG Ling-yu, NOEL S, JAJODIA S. Minimum-cost network hardening using attack graphs[J]. Computer Communications, 2006, 29(18):3812-3824.

[10] LIPPMANN R P, INGOLS K W, SCOTT C, *et al*. Evaluating and strengthening enterprise network security using attack graphs, ESC-TR-2005-064[R]. [S. l.]: MIT Lincoln Laboratory, 2005.

[11] SAWILLA R, OU Xin-ming. Googling attack graphs, TM-2007-205[R]. Ottawa: Defence R&D Canada, 2005.

[12] CNCERT/CC. CNCERT/CC annual report[R/OL]. (2004). http://www.cert.org.cn/.

[13] SWILER L P, PHILLIPS C, GAYLOR T. A graph-based network vulnerability analysis system, SAND97-3010/1 UC-705[R]. [S. l.]: Sandia National Laboratories, 1997.

[14] INGOLS K, LIPPMANN R, PIWOWARSKI K. Practical attack graph generation for network defense[C]//Proc of the 22nd Annual Computer Security Applications Conference. 2006.