基于漏洞关联攻击代价的攻击图生成算法*

何江湖[a], 潘晓中[a,b]

(武警工程大学 a. 电子技术系 网络与信息安全武警部队重点实验室; b. 信息安全研究所, 西安 710086)

摘 要: 在已有的网络攻击图生成方法的基础上,从漏洞关联的攻击代价出发,设计了一种攻击图生成基本框架,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。该算法能有效结合漏洞之间的相关性,科学地评估攻击代价,有效删除了攻击代价过高、现实意义不大的攻击路径,简化了攻击图,并通过实验检验了该算法的合理性和有效性。

关键词: 攻击图; 攻击代价; 漏洞关联; 自动生成

中图分类号: TP391 **文献标志码**: A **文章编号**: 1001-3695(2012)05-1907-03

doi:10.3969/j.issn.1001-3695.2012.05.082

Algorithm of attack graph generation based on attack cost of vulnerability relations

HE Jiang-hu[a], PAN Xiao-zhong[a,b]

(*a. Key Laboratory of Network & Information Security under the Chinese Armed Police Force, Dept. of Electronic, b. Institute of Information Security, Engineering University of Chinese Armed Police Force, Xi'an* 710086, *China*)

Abstract: On the basis of existing attack graphs generation methods, this paper took the attack cost of vulnerability relations as a point of departure to design a basic framework of automatic generation of attack graph and proposed an algorithm of attack graph generation based on the attack cost of vulnerability relations. By combining the correlation between vulnerability, this algorithm made a scientific evaluation of attack cost by effectively eliminating excessive attack cost and attack path with little significance. It also simplified attack graph and examined the rationality and validity of algorithm through experiment.

Key words: attack graph; attack cost; vulnerability relations; automatic generation

0 引言

随着计算机的普及、网络技术的飞速发展,社会和个人对网络信息的依赖性也日益增长,然而人们在得益于计算机和计算机网络的同时,也不得不面对信息安全问题带来的严峻考验。黑客入侵、病毒困扰给各行各业带来了巨大的经济和其他方面的损失。随着信息时代的到来,各种各样的信息战、电子战也越演越烈,并逐渐成为了国家与国家、企业与企业、公司与公司之间的竞争手段之一。因此,网络安全问题已经成为了影响全国、全世界以及各行各业的重大问题。

基于上述原因,网络安全问题近年来受到了极大的重视并以飞快的速度发展,特别是一些与之相关的,如网络攻击、入侵检测、防火墙等技术,不断地得到了更新与提高。随着信息化的不断推进,网络攻击手段也呈现出复杂化和多样化。是否能够及时发现网络状态的变迁和存在的攻击序列,已经成为了确保网络安全的一个重要环节。因此,研究人员适时提出了攻击图的概念。网络攻击图就是一组攻击者能够使目标计算机网络系统的特定安全属性遭受破坏的攻击预案集合。它将网络拓扑信息考虑在网络建模工作中,通过模拟攻击者对存在安全漏洞的网络的攻击过程,找到所有能够到达目标的攻击路径,同时将这些路径以图的形式表示[1]。而对网络攻击图的自动生成模型的研究,更是使得攻击图的建模和评估工作减少了人为的主观因素影响,变得更加科学化、客观化。通常攻击图只有一个初始状态,目标的状态可以是多样的。目标状态是由攻击者的类型以及攻击者所要达到的目的所决定的。

攻击图是由 Cunningham[2] 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。攻击图的边用来表示攻击者所要付出的攻击代价,也就是攻击所要花费的费用。而最早提出生成完整攻击图方法的是 Kuang[3],并在后来的研究工作中逐渐扩展成一种网络环境——NetKuang 系统,该系统主要是用来分析 UNIX 主机的网络配置脆弱性。Sheyner 等人[4] 提出了一种基于模型检测的网络攻击图自动生成方法,这是一种在攻击图上进行的网络安全分析,但这种方法存在系统状态空间大且呈指数增长等问题。Man 等人[5] 针对攻击图的生成状态复杂的问题,提出了一种基于宽度优先搜索的全局攻击图生成算法,通过限制攻击步骤和攻击路径的成功概率来减少攻击图的复杂性。李赓等人[6] 针对网络攻击图算法攻击路径不明确、状态空间过大等问题严重影响到攻击图在网络攻击与网络安全分析过程中不能很好应用的问题,提出了一种基于精简状态空间的改进算法,该算法通过限制网络的状态空间,使得生成的路径比较明确,并且使得攻击图的状态空间得到有效的控制。宋舜宏等人[7] 根据

收稿日期: 2011-09-23; **修回日期**: 2011-10-30 **基金项目**: 陕西省自然科学基金资助项目(2010JM8034);武警工程大学基金资助项目(wjy201027)

作者简介: 何江湖(1985-),男,广东茂名人,硕士,主要研究方向为网络攻防(hjh7510@126.com);潘晓中(1964-),男,陕西西安人,教授,主要研究方向为网络安全与信息安全.

网络攻击者总是希望更快地进入到网络内部,能够直接访问更加重要的主机,从而获得更高的主机访问权限这一前提,分析了各种攻击过程的贪心策略,构建了一种基于贪心策略网络攻击图的生成方法。

本文从攻击者为了达到攻击目的,采取各种各样的攻击手段所可能要经过的攻击路径和攻击状态转移的角度出发,设计了一种攻击图的自动生成系统基本框架,并根据漏洞关联关系和攻击时所要付出的代价,设计了一种带攻击代价的攻击图生成算法。

1 攻击图生成系统的基本框架

攻击图的生成是通过对攻击的模拟得出来的。在模拟时,首先要确定攻击者的目的,不同攻击者的目的是不同的,生成的攻击图也不同。对于一个特定系统来说,它存在的危险是一定存在的,相比文献[8],本文在攻击图生成系统框架中加入了网络知识安全库,并对攻击图生成系统的基本框架进行了完善与改进。

本文攻击系统的基本结构如图 1 所示。通过网络扫描器对目标计算机和网络进行扫描并获得相关数据,如主机配置、网络情况、系统类型等信息,添加到系统的状态队列。当攻击图生成系统空闲时,自动从系统状态队列当中抽取一种状态信息,送入网络知识安全库模块进行比较。网络安全知识库检验该信息为不安全时,则分析该信息,确定漏洞特征,记录在漏洞列表库中。攻击特征库对漏洞列表库的漏洞特征进行提取与总结,并参考网络安全知识库,得出该信息的攻击特征,最终确定其危害性。攻击推论引擎根据攻击特征库生成攻击图,并通过可视化工具输出攻击图。攻击推论引擎包含了生成基本攻击、生成攻击图两个主要部件,实现对攻击特征库信息的攻击模拟,这些信息包括原子攻击集合、攻击者的初始状态与目标状态、原子攻击选择策略、主机可达性以及搜索策略等。通过建立网络知识安全库,可以加快发现主机或网络当中的不安全因素,提高系统发现不合法信息的速度,并实现攻击的自动检测与攻击图的自动生成。

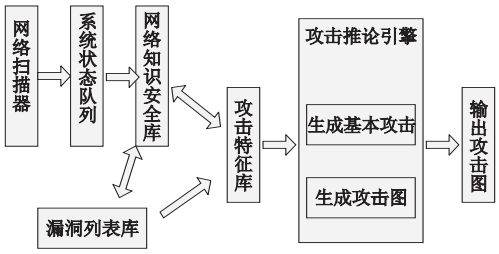

图1 攻击图生成系统的基本框架

2 攻击图生成算法描述

网络攻击图是一种描述不同攻击之间关联性的模型,能更好地描述攻击者所采取攻击步骤对目标资源实施的攻击行为,因此,与只针对孤立漏洞进行扫描分析的方法相比,借助攻击图能更准确和更有效地评估网络或系统的安全[9]。它是为发现网络中复杂的攻击路径或者引起系统状态变迁的渗透序列,是通过模拟攻击目标主机漏洞和网络连接关系等因素提出的,用于描述网络安全状态的一种方法。文献[10]提出攻击图中包含属性节点和原子攻击节点两类。原子攻击节点代表攻击者利用单个脆弱性进行的一次攻击。属性节点代表目标网络、攻击者能力的条件,攻击图的每条边代表一个单一行为引起的状态改变,行为的执行者可能是攻击者、普通用户、后门程序等。攻击图的生成算法有两个阶段,第一阶段是进行信息收集,它的任务是收集攻击的网络主机的配置情况、网络类型与网络弱点等;第二阶段是对攻击行为的可能性进行模拟。目前对于攻击图的生成方法有很多,已有一些较为成熟的攻击图生成方法,但是它们对于攻击图的代价利害关系、漏洞与漏洞之间的联系没有加以考虑。

漏洞是影响目标安全的一个重要因素,漏洞攻击代价主要由困难程度 D、隐蔽程度 C、花费时间 T 和期望收益 I 四个特点决定。通过结合网络部署情况、目标计算机弱点等实际环境的具体信息,对漏洞的各个特点攻击代价进行赋值,如表 1 所示。

表 1 漏洞的特点及赋值

漏洞特点	描述	赋值
困难程度 D	困难	9
	一般	6
	容易	4
隐蔽程度 C	攻击时很难被发现	9
	攻击时可能被发现	7
	攻击时容易被发现	2
花费时间 T	较长	8
	中等	6
	较少	3
期望收益 I	高	9
	中	6
	低	4

单个漏洞的攻击代价为 $V=\lambda_1 D+\lambda_2 C+\lambda_3 T+\lambda_4 I$。其中:$\lambda_1$、$\lambda_2$、$\lambda_3$、$\lambda_4$ 为对应的权值,在实际应用当中,可根据实际情况灵活选取。不同的攻击者在取值时所考虑的因素不同,如低水平的攻击者会更多地考虑攻击困难程度,而高水平的攻击者会更多地考虑攻击的隐蔽程度和攻击花费时间。

本文算法通过限定最大攻击代价,可以在攻击图生成过程中减少攻击代价过高的边,缩小攻击图的规模;而通过限定攻击深度,可以减少攻击深度过深、攻击意义不大的攻击路径,简化了攻击图。本文设计的算法描述如下:

```
算法:network_generate
输入:网络扫描目标机器信息,攻击代价 Attack_value,攻击深度
      Attack_depth。
输出:网络攻击图。
begin:
Queue State = new Queue;//建立网络状态队列
Attack_value = V;//攻击代价等于扫描代价
Attack_depth = 0;//攻击深度初始值为 0
State enQueue( init state);//将初始状态加入到队列当中去
while( State is empty( ))//当队列为空时执行循环
{
Nowdo queue( State);//从队列中取出一组节点数据
if( match( Nowdo, network_secure)
//将信息与网络安全知识库进行比较
{extend hole-list;//添加到漏洞列表库
  Preattack_value = Attack_value;
  Attack_value = V;//攻击代价等于扫描代价
  Attack_value = Attack_value + Preattack_value * relation;/ * 当前
的攻击代价为单个漏洞攻击代价加上上一步漏洞攻击代价乘以它们的
互相关系数 * /
  if{ Attack_value < = givemark; Attack_depth < = givelevel}/ * 当攻击
的单边代价权重小于等于某一个设定值且攻击深度不大于某个深度,
进行以下操作,否则丢弃 * /
  Attackdepth + + ;//攻击深度加 1,表示攻击图进一步向下扩展
  Graph. add ( Nowdo, Attack_value, Attack_depth);
```

```
//将当前节点添加到攻击图
}}
else drop;
esle{Nowdo queue(State);//从队列中取出另一组节点数据
}
```

3　实验

3.1　实验环境

为了验证本文算法的有效性及合理性,本文构造了一个网络模拟实验环境,其拓扑结构如图 2 所示。

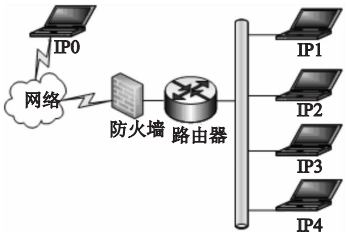

图2　网络拓扑结构

在模拟实验环境中共有四台主机,并且在同一网段,它们之间通过路由器进行通信联络,整个网络通过防火墙与外界隔开。IP0(攻击者)位于 Internet 中,其攻击目的是获取内网中的 IP4 主机的 root 权限从而窃取存储在其上的重要资料。在内网中,IP1 主机开放了 Telnet 服务、IP2 主机运行的是 SMTP 服务器,开放了 FTP 服务;IP3 主机运行 MySQL 数据库和开放 HTTP 服务;IP4 主机开放 SSH 服务并且存储重要的资料。防火墙只允许外部主机访问主机 IP2 上的 FTP 服务,其他的外部访问均被阻止,内部网络之间互访没有任何限制,也就是说网络内部主机可以访问内部网络中存在的任何远程服务。

在实验开始时,攻击者对实验环境网络内各主机信息和存在的漏洞进行收集,如表 2 所示。通过对漏洞进行分析研究,根据实际情况进行赋值,并结合第 2 章的单个漏洞攻击代价生成公式,计算得出单个漏洞攻击代价,如表 3 所示。每个漏洞之间的相关系数如表 4 所示。

表2　主机信息

hosted	service	vulnerability ID
IP1	Telnet	12410
IP2	SMTP,FTP	11542
IP3	MySQL,HTTP	11565,8952
IP4	SSH	10807

表3　漏洞攻击代价表

vulnerability ID	*V*
12410	40
11542	20
11565	60
8952	30
10807	80

表4　漏洞之间互相关系数

vulnerability ID	vulnerability ID	relative	vulnerability ID	vulnerability ID	relative
12410	11542	0.5	11542	8952	0.5
12410	11565	0.6	11542	10807	0.2
12410	8952	0.3	11565	8952	0.1
12410	10807	0.1	11565	10807	0.2
11542	11565	0.4	8952	10807	0.1

3.2　实验结果

为了方便实验和有效简化攻击图生成的规模,在实验验证本文算法时限定网络攻击图的攻击深度为 5,单边攻击最大代价为 100,使用设计的攻击图生成算法生成攻击图如图 3 所示。

3.3　实验分析

该算法通过对漏洞客观评价并赋值,使得攻击者可以根据生成的攻击图对攻击所付出的攻击代价有一个客观的初步了解,并可以根据攻击图对攻击路径进行最佳选择。根据图 3 的网络攻击图,攻击者可以轻松地找到本模拟实验环境下攻击代价最小的路径 IP0→IP1→IP4,总攻击代价为 124。通过限定单边的最大攻击代价,可以有效减小网络攻击图的生成规模,简化攻击图。网络安全人员也可以在对网络攻击图进行分析后,有针对性地采取相关措施,提高网络的安全性。

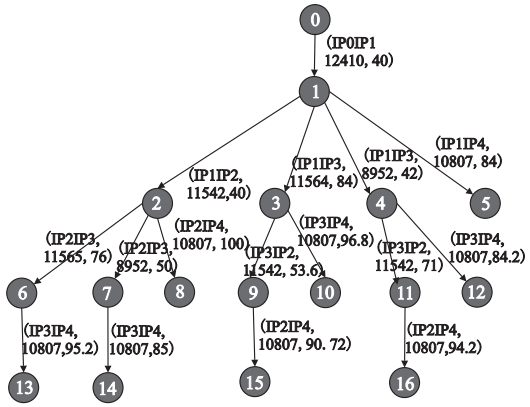

图3　算法生成的攻击图

4　结束语

目前网络攻击图的研究非常广泛,它是网络安全评估和测试的重要手段之一,网络攻击图的研究对网络安全工作有着十分重要的意义。本文针对网络攻击图自动生成的需求,提出了一种网络攻击图生成的基本框架,并根据漏洞关联特点,设计了一种带攻击代价的攻击图生成算法。该算法在一定程度上减少了网络爆炸问题,有效地去除了攻击代价大的边和节点,简化了网络攻击图的生成。下一步研究的重点主要集中在生成框架中网络安全知识库的优化及如何更加客观地生成算法中的漏洞攻击代价等问题。

参考文献:

[1] 王国玉,王会梅,陈志杰,等. 基于攻击图的计算机网络攻击建模方法[J]. 国防科技大学学报,2009,31(4):74-79.

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

[3] DANFORTH M. Models for threat assessment in networks[D]. Davis: University of California Davis,2006.

[4] SHEYNER O, HAINES J, JHA S, *et al*. Automated generation and analysis of attack graphs[C]//Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society, 2002: 273-284.

[5] MAN Da-peng,ZHANG Bing,YANG Wu,*et al*. A method for global attack graph generation[C]//Proc of IEEE International Conference on Networking,Sensing and Control. [S.l.]: IEEE,2008:236-241.

[6] 李虎,王祖林,赵毅寰. 基于精简状态空间的攻击图生成算法[J]. 计算机应用研究,2009,26(12):4747-4750.

[7] 宋舜宏,陆余良,夏阳,等. 基于贪心策略的网络攻击图生成方法[J]. 计算机工程,2011,37(2):126-131.

[8] 李玲娟,孙光辉. 网络攻击图生成算法研究[J]. 计算机技术与发展,2010,20(10):171-175.

[9] 吴金宇,金舒原,杨智. 基于网络流的攻击图分析方法[J]. 计算机研究与发展,2011,48(8):1497-1505.

[10] 陈锋,张怡,苏金树,等. 攻击图的两种形式化分析[J]. 软件学报,2010,21(4):838-848.