

网络攻击图生成算法研究

李玲娟, 孙光辉

(南京邮电大学 计算机学院, 江苏 南京 210003)

摘要:攻击模型能够对攻击过程进行结构化描述和有效分析,攻击图可以清楚地分析攻击者可能采取的攻击路径,两者对网络安全策略的制定具有重要的指导意义。设计了一种基于状态转移的网络攻击模型,并基于该模型设计了攻击图生成系统的架构和相应的攻击图生成算法,在攻击图生成算法中引入了代价分析机制和规模控制机制。仿真实验结果表明,利用所设计的模型和算法不仅能有效地预测攻击者可能采用的各种攻击路径和最佳攻击路径,而且能有效地控制攻击图的规模。

关键词:攻击模型;攻击图;状态转移;攻击代价分析

中图分类号:TP393

文献标识码:A

文章编号:1673-629X(2010)10-0171-05

Research on Algorithm of Generating Network Attack Graph

LI Ling-juan, SUN Guang-hui

(College of Computer, Nanjing University of Posts and Telecommunications,
Nanjing 210003, China)

Abstract: Attack model can help structurally describing and effectively analyzing the course of attack, and attack graph can clearly analyze the attack paths the attacker may take. Both of them play the guiding role for the establishment of network security policy. A network attack model based on state transition is designed, and a framework of the attack graph generation system as well as the algorithm of generating the attack graph is also designed. In the algorithm, attack costs are analyzed, and the method of controlling the graph size is adopted. The experiment result shows that the possible attack paths as well as the best attack path can be effectively doped out by the model and algorithm, and the graph size can also be controlled by them.

Key words: attack model; attack graph; state transition; attack costs analysis

0 引言

网络攻击过程是一个攻击者根据攻击条件和目标,通过过程实施进行信息获取和权限提升的过程,其攻击效果取决于攻击者能力、经验与其支配环境^[1]。常用的网络攻击手段有很多,如端口扫描、拒绝服务攻击、病毒攻击、特洛伊木马、恶意代码、缓冲区溢出、口令破译等。

网络攻击发生的前提条件是网络(或系统)中存在着弱点,由于这些弱点之间存在着一定的关联性,主机设备也存在着相互信任关系,网络攻击者可以利用这些关联性或信任关系,在一次具体攻击完成后,进行后续攻击。因此,网络攻击通常是一种复杂的多步骤的

过程,一次完整的攻击过程通常会包括一系列单独的攻击行为,发生在不同的网络部分却又相互关联。

对于网络管理者,如果能够提前获知或预测可能发生的攻击序列(攻击路径),就可以及时采取预防措施,提高网络的安全性,减少网络攻击的发生。为此,如何合理地描述攻击相关联的行为,进而有效地组织这些行为,提高模拟网络攻击的效率,已成为网络攻击方面的一大研究热点。

目前对网络攻击方法进行模型描述的主要手段有^[2]:攻击描述语言、攻击树、攻击图、攻击网。这些手段能对网络攻击很好地描述,对构建攻击系统也有很好的指导作用。而在攻击模型和攻击算法方面,已产生了一些较好的研究成果^[3-6],但仍存在一些问题需要进一步研究和改进。

文中以有效地预测攻击者可能采取的攻击路径为目的,设计了一种基于状态转移的网络攻击模型,并基于该模型设计了一个攻击图生成系统的架构和一种基于代价分析的攻击图生成算法。

收稿日期:2010-02-08;修回日期:2010-05-17

基金项目:国家863计划(2006AA01Z439);江苏省高校自然科学基金研究项目(08KJB620002);南京邮电大学校科研基金(NY207051)

作者简介:李玲娟(1963-),女,辽宁辽阳人,教授,研究方向为数据挖掘、网络安全等。

1 基于状态转移的网络攻击模型

文中设计的基于状态转移的网络攻击模型的基本思想是:将一次成功的网络攻击行为(原子攻击)抽象成对网络状态的一种改变,以此形成反映攻击路径的攻击图。具体模型见图 1。

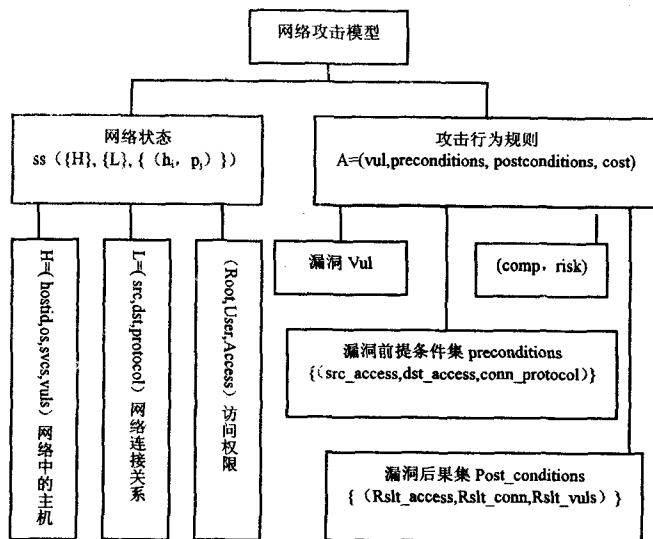


图 1 基于状态转移的网络攻击模型的构成
攻击模型由网络状态和攻击行为规则两个属性构成。

本模型中的网络状态(system status)表示为 $ss(\{H\}, \{L\}, \{(h_i, p_i)\})$ 。其中 $\{H\}$ 为主机的集合,网络中的主机是网络中的基本元素,用四元组 $H=(hostid, os, svcs, vuls)$ 来表示。其中 $hostid$ 是主机在网络中的唯一标识符,可以用 IP 地址来表示; os 是主机所运行的操作系统及其版本信息; $svcs$ 表示主机所开放的服务列表,可用端口号表示; $vuls$ 是主机上的弱点列表,弱点包括操作系统的弱点、主机所安装的软件弱点、其他一些错误配置信息等。 $\{L\}$ 为网络连接关系的集合,网络连接用一个三元组 $L=(src, dst, protocol)$ 来表示。其中 src 表示源主机, dst 表示目标主机, $protocol$ 表示主机间连接的协议或者端口。若二者不存在连接关系时, $protocol$ 为空集,当二者为同一主机时, $protocol = \{localhost\}$ 。 $\{(h_i, p_i)\}$ 为攻击者对网络中各主机的访问权限集合,表示用户在主机 h_i 上具有访问权限 p_i 。本模型将权限分为三级:系统管理员级 $Root$,它对主机资源有完全控制能力;普通系统用户级 $User$,它由系统初始化产生或系统管理员创建,有自己私有的资源;可以访问网络服务的远程访问者级 $Access$,它能和网络服务进程数据交互,可以扫描系统的信息。

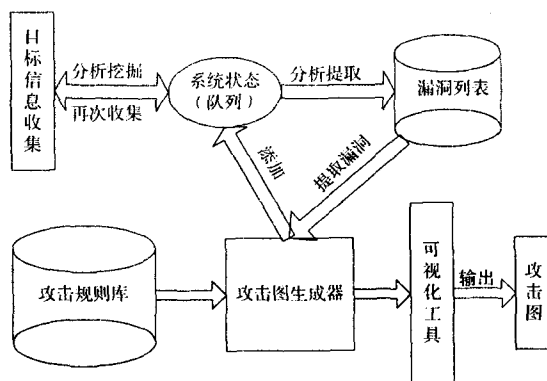
本模型中的攻击行为规则可以用四元组表示为 $A=(vul, preconditions, postconditions, cost)$ 。将攻击者的一次攻击行为看成是对弱点的一次利用,其结果可以

看作是一次攻击权限的提高或者连接关系的增加或者弱点的增多。其中, vul 表示攻击所利用的弱点, $preconditions$ 为利用此弱点必须满足的前提条件的集合,包含三个元素($src_access, dst_access, conn_protocol$), src_access 表示攻击者在攻击源主机上应具有的最小访问权限, dst_access 表示攻击者在目标主机上应具有的最小访问权限, $conn_protocol$ 表示攻击源主机与目标主机之间应满足的连接关系。 $postconditions$ 表示攻击行为导致的后果的集合,用三元组 ($Rslt_access, Rslt_conn, Rslt_vuls$) 表示。其中, $Rslt_access$ 表示当攻击行为成功完成后,攻击者在目标主机获得的访问权限, $Rslt_conn$ 表示攻击行为成功完成后,网络连接关系的改变, $Rslt_vuls$ 则表示攻击行为成功完成后所增加的弱点。 $cost$ 表示攻击行为完成所花费的代价,由攻击复杂度以及攻击被发现的风险两部分组成,用二元组 $cost=(complex, risk)$ 来表示。

2 攻击图生成系统的基本架构

网络攻击图被用来反应网络中各种弱点的关联性,借助攻击图可以清楚地分析攻击者可能采取的 attack 路径。文献[7]最先提出了攻击图概念,用攻击图的节点表示可能的攻击状态,节点内容通常包括主机名、用户权限、攻击的影响等;每条边代表一个单一行为引起的状态改变,行为执行者可能是攻击者、普通用户、后门程序等。

文中基于图 1 的攻击模型和上述的攻击图概念,设计了图 2 所示的攻击图生成系统架构。



在目标信息收集模块,通过各种扫描、探测以及其他技术对目标系统进行信息收集;对收集到的信息进行分析挖掘,按照上述模型,得出系统状态,系统状态可能需要经过多次收集才能最终确定;从系统状态提取出在此状态下存在的每个弱点,形成弱点列表,弱点列表表示在当前系统状态下,所有弱点的集合;然后,

在攻击图生成器中,运行攻击图生成算法生成攻击图,这也是攻击图生成系统的核心部分;最后,通过可视化工具展示攻击图。所生成的攻击图中,节点表示网络状态,边表示攻击行为。节点之间用有向边相连接,表示在一种攻击行为下,系统由一种状态向另一种状态转移。

3 基于代价分析的攻击图生成算法

目前,已有一些较为有效的攻击图生成方法,但他们对攻击图规模的控制未加考虑。

文中则在注重算法效率的同时,充分考虑攻击图的规模,设计了一种基于代价分析的攻击图生成算法,该算法做了两点假设:

(1)假设攻击者的能力足够强,在已满足攻击前提条件的情况下,攻击行为都能够成功完成。

(2)假设每次攻击行为成功完成后,都能导致攻击者后续攻击能力的提高,即每次攻击都能导致攻击者访问权限的提升,或者网络连接关系的增加,或者弱点的增多。

尽管不一定所有的攻击者都能完成相应的攻击,但对于网络管理者来说,所有有可能完成的攻击,对于网络系统的威胁都是潜在的,为了最大化发掘系统存在的风险,做了第一条假设。做第二条假设的目的是将系统空间限制在一定范围内,避免其无限增大。

3.1 算法描述

基于代价分析的攻击图生成算法用正向广度优先搜索算法生成攻击图,使用队列结构来保存每次产生的新节点。

算法的基本思想是:首先将网络初始状态加入队列,然后执行循环:从队列中取出一种状态节点,考察节点的深度以及代价,若没有超出预设阈值,则对该状态下每一弱点,判断攻击前提条件是否成立,如果成立则生成新状态节点并加入队列。然后再从队列中取新节点,直到队列为空,循环结束。具体算法如下:

算法:GenerateGraph

输入:网络初始状态:init_state

最大攻击深度:MaxDepth

最大攻击代价:MaxCost

输出:攻击图:Attack Graph

过程:

Begin:

Queue State_queue = new Queue; //建立网络状态队列

State_queue <- EnQueue(init_state); //将初始状态加入队列

While(State_queue.IsEmpty()) //队列非空时执行循环

{ N_current <- dequeue(State_queue); //从队列中取出一种状态

if (N_current != N_goal && N_current.depth < MaxDepth && N_current.cost < MaxCost) // N_current 指当前节点, N_goal 指目标节点

{for each vul in N_current.vuls //对于当前状态的每一个弱点考察攻击规则库

{ if(A.preconditions = true) //如果前提条件满足,根据规则库中该行为导致的后果,生成新状态节点 N_ss

{N_ss.depth = N_current.depth + 1; //计算当前节点深度

N_ss.cost = N_current.cost + cost; //计算当前节点代价

Graph.Addedge(N_current, N_ss); //生成以当前节点 N_current 为起点, N_ss 为终点的边,并加入到图中

State_queue <- EnQueue(N_ss); //新节点 N_ss 入队列

}}}}

3.2 算法分析

(1)攻击图规模的控制措施。

有些攻击图生成算法存在状态爆炸问题(例如文献[8]的算法),当主机超过一定数量时,会使攻击图规模过大、生成过程耗时过长。

本算法通过两种途径来解决以上问题。其一是限制攻击路径的深度,也就是攻击序列的长度;这是因为在攻击图的生成过程中,攻击深度每增加一步,就会带来攻击图规模的指数级增长。其二是在攻击图的生成过程中,计算所生成节点的代价,对于超过代价阈值的节点,认为攻击代价过大,攻击不能完成,便不再生成其后继节点,以此减少攻击图中无效节点的数量。

(2)攻击路径的代价分析方法。

在对每条路径的代价分析中,做了以下三个方面的考虑:

①考虑攻击序列中的每个子攻击代价。

这个代价由攻击的复杂度决定。弱点的攻击复杂度是对攻击者成功利用某一弱点难易程度的度量,它受多种因素的影响,例如攻击工具的自动化程度、攻击时间和攻击者的经验等。精确地描述各个弱点的攻击复杂度是不可能的,只能通过一些变量来近似地表达出不同弱点之间攻击复杂度的差别。研究人员通过对大量安全事件的调查和统计^[9],发现弱点的发掘利用周期和攻击复杂度之间存在一种映射关系,通过这种

映射关系能够表达出各个弱点在攻击复杂度上的差异。在此基础上,文献[10]对 Internet 上已公开的几百种弱点的利用方法和攻击工具进行了分析和比较,给出了攻击复杂度的量化标准,文中对其进行了修改和完善,修改后的量化标准如表 1 所示。

表 1 弱点攻击复杂度量化表

等级	复杂度	描述
1	0.1	无需攻击工具,有详细的攻击方法
2	0.3	有现成可用攻击工具和详细攻击方法
3	0.5	无攻击工具但有较详细的攻击方法
4	0.7	公开报告此弱点,粗略提及攻击方法
5	0.9	公开报告此弱点,未给出攻击方法

将一条攻击路径中每步的攻击代价记为 comp_i ($1 \leq i \leq n$) (其中 i 表示当前攻击路径深度, n 为总的攻击路径的长度)。此时若不考虑其他方面,一个攻击序列或攻击路径的攻击代价可记为:

$$\text{cost} = \sum_{i=1}^n \text{comp}_i$$

② 进一步考虑前后攻击所需代价的关系。

若一条攻击路径上存在针对同一弱点发生的攻击行为,则后面的攻击行为看成前面攻击行为的相似攻击。那么这时可以考虑后一次攻击行为所需要的代价将比前面的所需代价小。因为有了前面攻击的影响和攻击者经验的积累,后面相似行为进行起来会更容易。因此,整个过程的攻击代价可以改写为:

$$\text{cost} = \sum_{i=1}^n (X_i^{\text{time}-1} * \text{comp}_i)$$

其中 X_i ($X_i < 1$) 表示攻击过程对攻击者经验的依赖系数,文中设为 0.5,表示第二次相似攻击代价为原代价的一半;time 表示攻击过程相似子攻击的重复次数。

③ 进一步考虑攻击暴露风险代价。

由于每进行一次攻击,都可能被网络管理员或者入侵检测系统发现,所以,网络攻击路径代价的计算还需考虑风险代价。由于入侵检测大多是根据入侵行为表现出来的一系列特征来判断是否发生入侵行为,因此随着攻击路径的深入,其暴露出来的特征越多,也就越容易被发现,而且每深入一步,其代价将呈指数增加。因此,考虑将攻击路径深度作为风险代价评估的因素。这里,再次将攻击代价改写为:

$$\text{cost} = \sum_{i=1}^n (X_i^{\text{time}-1} * \text{comp}_i * \theta_i^i), \theta_i (\theta_i > 1)$$

θ_i 表示风险系数,由专家经验决定,文中设定为 2,表示每深入一步,花费代价增长一倍。可以由此式计算每条攻击路径所花费的代价,从而获取最佳的攻击路径。

4 仿真实验

4.1 实验环境

为了验证以上各项设计的有效性,文中做了仿真实验。实验中参考了文献[11]和文献[12]提供的数据和函数,实验采用的网络拓扑结构如图 3 所示。

网络中有五台计算机,IP1、IP2、IP3、IP4 和 IP5,它们在同一网段内通过路由器相连,通过防火墙与外界隔开。IP1、IP2 都是 Linux 主机,IP3、IP4 和 IP5 都是 Windows 主机。

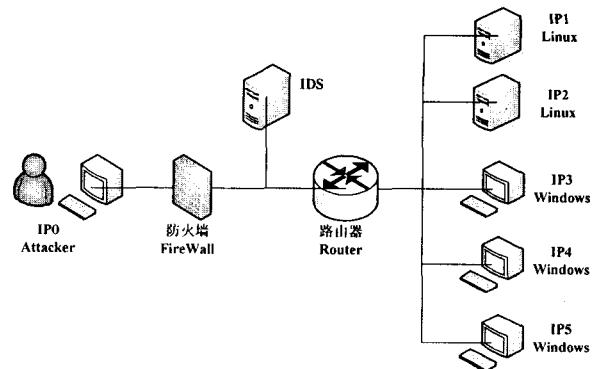


图 3 实验网络拓扑结构

在实验中,IP1 开放 FTP 服务和 SMTP 服务,IP2 开放 HTTP 服务,IP3 开放 FTP 服务,IP4 开放 Telnet 服务和 SSH 服务,IP5 是关键主机,其上存储重要资料。外网的入侵者位于 IP0 主机上,并且对自己的主机 IP0 拥有 Root 权限。防火墙的访问策略是允许外部主机对 IP2 的 HTTP 服务进行访问,其它访问均被阻止。这样,攻击者只有对 IP2 的访问权限,其他均被限制。每台主机存在的弱点及其弱点复杂度信息见表 2 和表 3。

表 2 主机描述表

hostid	os	svcs	vuls
IP1	Linux	FTP,SMTP	{15343,8641}
IP2	Linux	HTTP	{11964}
IP3	Windows	FTP	{11826,8826}
IP4	Windows	Telnet,SSH	{12815,6247}
IP5	Windows		{10707}

表 3 弱点复杂度量化表

Bugtraq ID	复杂度
15343	0.1
8641	0.3
11964	0.7
11826	0.5
8826	0.3
12815	0.5
6247	0.7
10707	0.5

4.2 实验结果与分析

首先,在没有任何限制条件下生成了一个完整的攻击图,图中有 106 个节点和 105 条边,其中可以到达攻击目标的攻击路径共有 46 条。

接着,用文中设计的算法,设定最大攻击深度为 5、最大攻击代价为 5,产生的攻击图见图 4。

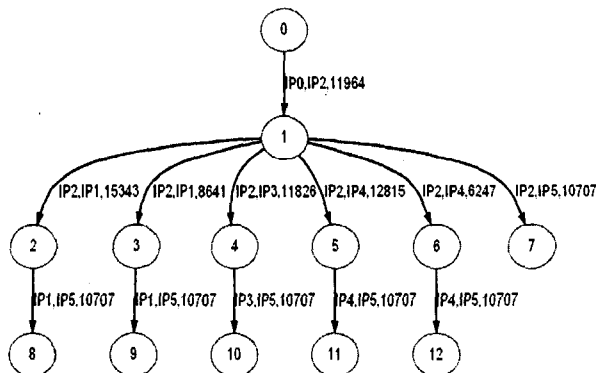


图 4 最大深度 5、最大攻击代价 5 的攻击图

图 4 共有 13 个节点和 12 条边,其中可以到达攻击目标的路径有 6 条,各路径及代价见表 4。

表 4 攻击路径代价表

编号	实际路径	代价
1	(IP0, IP2, 11964)→(IP2, IP1, 15343)→(IP1, IP5, 10707)	2.9
2	(IP0, IP2, 11964)→(IP2, IP1, 8641)→(IP1, IP5, 10707)	3.3
3	(IP0, IP2, 11964)→(IP2, IP3, 11826)→(IP3, IP5, 10707)	3.7
4	(IP0, IP2, 11964)→(IP2, IP4, 12815)→(IP4, IP5, 10707)	3.7
5	(IP0, IP2, 11964)→(IP2, IP4, 6247)→(IP4, IP5, 10707)	4.1
6	(IP0, IP2, 11964)→(IP2, IP5, 10707)	1.7

运行文中的算法后,攻击图的规模被有效地控制,明显减小。

另外,由表 4 可知,路径(IP0, IP2, 11964)→(IP2, IP5, 10707)代价最小,攻击者最容易从该路径入侵;同时每条攻击路径都利用了弱点 11964 和弱点 10707。因此,管理员可以据此采取相应的措施,防止攻击者的入侵。

5 结束语

目前,网络安全管理是一项具有挑战性的工作,保

护网络安全必须对网络攻击技术进行深入的研究。文中研究了攻击模型、攻击图生成等与网络攻击技术有关的内容,着重研究了攻击图生成算法。并通过实验证明了所设计的基于状态转移的攻击模型及基于代价分析的攻击图生成算法可以较为有效地预测攻击者可能采取的所有攻击路径和最佳路径,从而为防范攻击提供依据。

参考文献:

- [1] 陈春霞,黄 皓. 攻击模型的分析与研究[J]. 计算机应用研究,2005,22(7):115-118.
- [2] 张森强,唐朝京. 基于攻击效能的网络攻击法分类与形式化描述[J]. 信息与电子工程,2004,2(3):161-166.
- [3] Jan S, Markus S. Collaborative Attack Modeling[C]// Proceedings of the 2002 ACM Symposium on Applied Computing. New York, NY, USA:ACM,2002:253-259.
- [4] Andrew M, Robert E, Richard L. Attack Modeling for Informational Security and Survivability[DB/OL]. 2001-03. <http://www.cert.org/archive/pdf/01tm001.pdf>.
- [5] 司加全,张 冰,苟大鹏,等. 基于攻击图的网络安全性增强策略制定方法[J]. 通信学报,2009,30(2):123-128.
- [6] 苟大鹏,张 冰,周 渊,等. 一种深度优先的攻击图生成算法[J]. 吉林大学学报(工学版),2009,39(2):446-452.
- [7] Phillips C, Swiler L P. A graph-based system for network vulnerability analysis[C]// Proceedings of the NSPW'98. New York, NY, USA:ACM,1998:71-79.
- [8] Swiler L P, Phillips C, Ellis D, et al. Computer-attack graph generation tool[C]// Proceedings of the DISCEX II'01. Albuquerque, NM:Sandia Nat. Labs.,2001:307-321.
- [9] Browne H K, Arbaugh W A. A Trend Analysis of Exploitations[C]// Proc. of 2001 IEEE Security and Privacy Conference. Oakland, USA: IEEE Press, 2001:214-229.
- [10] 张永铮,云晓春,胡铭曾. 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,2004,25(7):107-114.
- [11] Bugtraq. Security Focus[EB/OL]. 2009-03. <http://www.securityfocus.com/archive/1>.
- [12] Graphviz. Graph Visualization Software[EB/OL]. 2009-06. <http://www.graphviz.org/>.

(上接第 170 页)

- [8] 李 频. 虚拟专用网的主要隧道协议的安全性剖析[J]. 计算机工程,2002,32(13):164-169.
- [9] 戴宗坤,唐三平. VPN 与网络安全[M]. 北京:电子工业出版社,2002.
- [10] Ferguson N, Schneier B. A Cryptographic Evaluation of IPSec

- [R]. [s.l.]:Counterpane Internet Security Inc.,2003.
- [11] 沈 莉. IPv6 的安全协议研究[J]. 电子科技大学学报,2002,31(1):72-75.
- [12] Yuan Ruixi, Strayer W T. Virtual Private Networks: Technologies and Solutions[M]. Boston: Addison Wesley Publishing Company, 2002.