文章编号:1673 - 0062(2014)03 - 0082 - 05

基于有序搜索的攻击图生成算法

刘芳菊[1],林睦纲[2],谭敏生[1*]

(1. 南华大学 计算机科学与技术学院,湖南 衡阳 421001;2. 衡阳师范学院 计算机科学系,湖南 衡阳 421008)

摘 要:为了有效的生成攻击图并且限制攻击图的规模,提出基于有序搜索的攻击图生成方法. 该方法采用估价函数作为网络状态节点拓展的依据,估价函数值越小,优先进行扩展. 利用该方法降低网络攻击图的规模,减少系统生成攻击图时耗费的资源,生成的攻击图能够用于评估网络的安全性,能够给网络管理员提供有价值的信息用于管理网络,预防入侵.

关键词:攻击图;有序搜索;网络安全

中图分类号:TP393.08 **文献标识码**:A

Generation Algorithm of Network Attack Graph Based on Sequential Search

LIU Fang-ju[1], LIN Mu-gang[2], TAN Min-sheng[1*]

(1. School of Computer Science and Technology, University of South China, Hengyang, Hunan 421001, China; 2. Department of Computer Science, Hengyang Normal University, Hengyang, Hunan 421008, China)

Abstract: In order to effectively generate the attack graph and limit the scale of the attack graph, a generation algorithm of network attack graph based on sequential search is presented. This method extends network state nodes in according with the estimate function when generating attack graph, and the node with less estimate function value extends first. The method can reduce the scale of attack graph effectively and save the resource of computer to generate graph. We can assess the security of networks by the attack graph generated in this way, and provide valuable information for network administrator to manage networks and prevent attacks.

key words: attack graph; sequential search; network security

收稿日期:2014 - 03 - 20

基金项目:国家自然科学基金资助项目(11171095;61300234);湖南省教育厅科研基金资助项目(14A121;10C1147)

作者简介:刘芳菊(1974 -),女,湖南衡阳人,南华大学计算机科学与技术学院讲师,硕士. 主要研究方向:网络安全,智能计算. *通信作者.

0 引　言

随着计算机的普及和网络的飞速发展,网络安全已成为人们日渐关注的问题. 网络安全防御不仅仅包括发现和修复漏洞,还应该包括整个网络有效的安全评估与主动防御手段,建立起综合防御体系. 攻击图是综合考虑漏洞、攻击目标、主机和网络连接关系等安全状态,把攻击者可能的攻击路径以图的形式刻画出来,以便形象直观地理解目标网络内各个脆弱点之间的关系以及可能产生的威胁,为系统管理员理解攻击的特性,推测攻击者所有可能采取的攻击手段及攻击路径,决定应对措施的一种网络安全分析方法[1-5]. 通过攻击图能够遍历网络中所有可能存在的攻击,并发现在可能出现的多步攻击中的网络脆弱性,所以在多步攻击盛行的背景下,攻击图的研究已经成为网络安全研究的一大热点.

运用攻击图来研究网络安全,关键的一步就是攻击图的生成,然而攻击图的生成一直是攻击图研究的技术难点. 特别是随着网络规模的增大,在攻击图生成过程中可能产生状态爆炸问题,严重影响攻击图的实用性. 1998 年 Swiler 等人最初提出攻击图模型[6-7],该模型把攻击的状态和动作分别作为攻击图的节点和边,通过计算比较攻击成功的概率来获取关键的攻击节点,但生成攻击图的过程十分复杂. 为了简化生成攻击图的方法,许多学者提出基于模型检测技术(SMV/NuSMV)的自动生成攻击图的方法[8-10],该方法可很好地表示网络属性和攻击动作之间的依赖关系及攻击动作的时间顺序关系,但容易导致攻击图的规模较大、系统的状态空间较大. Ammann 和 Noel[11-12] 根据单调安全性假设来生成攻击图,极大地改善了问题的空间复杂性和时间复杂性,然而生成的攻击图包含大量的冗余路径,当网络较大时,生成的攻击图极其复杂. Noel[13] 等引入基于层次化约束过滤技术减少节点数量,运用交互邻接矩阵来简化网络配置的影响,增强了攻击图的可视性,但并不能解决状态空间爆炸问题. 文献[14]通过合并安全属性相同的主机来减少网络的状态空间,以达到避免状态空间激增的目的,但该方法只能局限地应用到集群网络环境. Dawkins[15] 等应用最小目标导出攻击链限制攻击树的规模,但由于该方法基于单一的目标,因此得到的攻击树可能存在非目标叶子节点. 近年来,许多学者运用各种算法来生成攻击图[16-21],其中许多算法是采用盲目搜索策略[17-19],由于搜索的盲目性而导致搜索的效率低,计算的时间与空间复杂性高,对于规模较大的网络,这样的算法无能为力.

有序搜索[22]是一种启发式搜索策略,在搜索过程中,它总是选择最有希望的节点作为下一个要扩展的节点,因此又称为最好优先搜索. 与盲目搜索相比,有序搜索减少了被扩展的节点数,从而缩小搜索范围,提高搜索效率. 特别在网络攻击中,攻击者往往选择最有希望的攻击路径进行攻击,基于这样一个事实和有序搜索的特征,本文将以状态转移的网络攻击模型为对象,运用有序搜索策略来设计一种有效的攻击图生成算法,有效地降低了攻击图的规模和系统生成攻击图时耗费的资源,在一定程度上避免了可能产生的状态爆炸问题.

1 攻击图建模

将攻击者每一次的攻击动作看作是一次网络状态的变迁,那么构造攻击图的过程是找出网络中潜在的渗透式攻击序列,从初始状态变换到目标状态的过程,帮助管理员更好的理解网络的安全状况. 本文采用文献[23]描述的网络攻击模型,攻击图模型有关的定义如下.

定义 1　攻击图:攻击图是一个状态转换系统 $T=(S,t,s_0,S_G)$,其中,S 是网络状态的集合,$t \subseteq S \times S$ 是状态转换关系的集合,$s_0 \in S$ 是网络初始状态,$S_G \subseteq S$ 是网络目标状态的集合. 网络状态一般包括当前网络中的主机状况,网络的连接关系及各用户权限.

定义 2　攻击路径:从初始状态 s_0 开始,若存在一组状态序列 $s_1,s_2,\ldots,s_{n-1}$,使得 s_0 过渡到目标状态 s_n,并且 $(s_i,s_{i+1}) \in t(0 \leqslant i \leqslant n-1)$,那么状态序列 $s_0,s_1,s_2,\ldots,s_{n-1},s_n$ 称为一条攻击路径.

定义 3　攻击行动:攻击行动用三元组(src_host,dst_host,vid)表示. 其中 src_host 是发动攻击的主机号,dst_host 是遭受攻击的主机号,vid 是此次攻击所利用的弱点号.

定义 4　攻击复杂度:弱点的攻击复杂度是用来衡量攻击者成功利用该弱点进行攻击的难易程度的一种度量. 弱点的攻击复杂度难以进行精确的量化,文献[24]对百种弱点的利用方法和攻击进行分析和比较,给出攻击复杂度的量化标准,见表 1.

表 1 攻击复杂度的量化标准

Table 1 Quantifying criteria of the exploitability

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

2 基于有序搜索的攻击图生成算法

如何有效地控制攻击图的规模,一直是攻击图生成研究中的重点和难点. 本文尝试应用有序搜索策略来生成攻击图,避免以往方法采用盲目搜索,搜索空间大,效率低的缺点. 该方法基于如下假设:攻击者有很强的攻击能力,能够实现对所有满足攻击条件的主机进行攻击,只是攻击者付出的代价不同而已. 实际上,不是所有的攻击都能完成,但对于网络管理员来说,任何潜在的危险都不应该放过,为了最大化发掘系统存在的风险,做以上假设.

2.1 基本思想

本文基于两种途径来解决攻击图生成的状态爆炸问题,以防主机增加到一定数目,攻击图的规模过大,生成攻击图的时间过长. 其一考虑攻击序列的长度,长度过长会使攻击图的规模呈指数级增长. 其二考虑攻击图生成过程中节点的代价,攻击成功所需要付出的代价太大,攻击者往往不会采纳,以此减少攻击图无效节点的数量,提炼攻击图的躯干,提醒网络管理员重点关注.

有序搜索是一种启发式搜索,在搜索过程中,它总是以最有希望达到最优目标的节点作为下一个扩展节点,不断地趋近最优值. 为了衡量节点的"希望"的启发信息,需要设计合适的估价函数,一个节点的希望程度越大,其估价函数值就越小,就越有可能被选为扩展节点,扩展节点选择估价函数最小的节点.

算法的基本思想是:采用估价函数 $f(n) = d(n) + \mathrm{cost}(n)$,其中 $d(n)$ 是攻击图中状态节点 n 的深度, $\mathrm{cost}(n)$ 用来计算状态节点 n 的代价. 构造 Open 表和 Closed 表,Open 表存储的是未扩展的节点,Closed 表存储的是已经扩展的节点,首先将网络初始状态加入 Open 表,然后执行循环:选取 Open 表中估价函数最小的节点扩展,对扩展节点判断每一弱点是否符合攻击条件,如果满足攻击条件,则把该节点加入 Closed 表,攻击者攻击该节点,生成新的状态节点,把新状态节点加入 Open 表中,然后又在 Open 表中选取估价函数最小的节点进行扩展,直到 Open 表为空或当前节点为目标状态节点.

2.2 算法描述

基于有序搜索的攻击图生成算法具体描述如下:

Step1)建立空的 OPEN 表和 CLOSED 表,把初始状态 S 加入 OPEN 表,并计算估价函数 $f(S) = \mathrm{cost}(S)$.

Step2)判断 OPEN 表是否为空表,如果为空表,则退出算法;如果不为空表,则重复执行下述操作:

Step2.1)从 OPEN 表中选择估价函数值最小的网络状态节点作为当前节点 N_{now};

Step2.2)如果当前节点 N_{now} 是目标节点 N_{goal},则退出算法,否则,重复执行执行如下操作:

Step2.2.1)把当前节点 N_{now} 移出 OPEN 表,并加入到 CLOSED 表;

Step2.2.2)对 N_{now} 节点中的每一个弱点,判断其是否符合攻击成功的前提条件,如符合,则执行下述操作:

Step2.2.2.1)根据攻击的结果,生成新的状态节点 N_{ss};

Step2.2.2.2)计算 N_{ss} 的估价函数值 $f(N_{ss}) = f(N_{\mathrm{now}}) + 1 + \mathrm{cost}(N_{ss})$;

Step2.2.2.3)若 N_{ss} 不在 OPEN 表和 CLOSED 表中,则把节点 N_{ss} 加入到 OPEN 表,并在攻击生成图中添加 N_{now} 指向 N_{ss} 的边 $N_{\mathrm{now}}N_{ss}$;

Step2.2.2.4)若 N_{ss} 已在 OPEN 表或 CLOSED 表中,则比较 $f(N_{ss})$ 与节点 N_{ss} 以前的估价函数值,若 $f(N_{ss})$ 小,则更新 N_{ss} 的估价函数值为 $f(N_{ss})$,在攻击图中删除 N_{ss} 与其父节点的边,添加 $N_{\mathrm{now}}N_{ss}$ 边,如果 N_{ss} 在 CLOSED 表中,则重新移回到 OPEN 表中.

3 仿真实验

3.1 实验环境

为了验证算法的有效性,仿真实验平台如图 1.

网络中有五台主机:IP1 到 IP5,这五台主机组成一个局域网,并通过路由器和防火墙接入到外网,攻击者位于外网. IP1 和 IP2 主机的操作系

统是 Linux,IP3,IP4 和 IP5 是 Windows 主机. 主机描述和弱点复杂度量化信息如表 2.

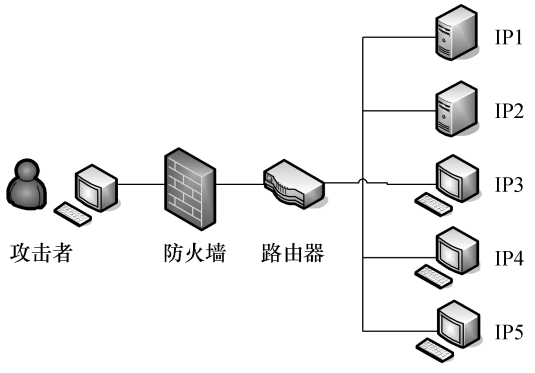

图 1　网络拓扑结构

Fig. 1　Network topology graph

表 2　实验主机和弱点信息

Table 2　Information of hosts and Vulnerabilities' information

主机	弱点号	范围	服务	权限	攻击复杂度
IP1	15343	远程	FTP	Root	0.1
	8641	远程	SMTP	User	0.3
IP2	11964	远程	HTTP	Root	0.7
IP3	11826	远程	FTP	User	0.5
	8826	本地	FTP	User	0.3
IP4	12815	远程	Telnet	User	0.5
	6274	远程	SSH	User	0.7
IP5	10707	本地		Root	0.5

表 2 中范围是指弱点的利用范围,权限是指攻击者成功攻击该弱点后可以获取的权限. 如表 2 所示,这五台主机的情况如下:主机 IP1 开放 FTP 服务和 SMTP 服务,主机 IP2 开放 HTTP 服务,主机 IP3 开放 FTP 服务,主机 IP4 开放 Telnet 服务和 SSH 服务,主机 IP5 存储大量重要信息,是攻击者攻击的目标. 局域网防火墙设置为:只允许外网访问主机 IP2 的 HTTP 服务,阻止外部其它的访问,局域网各主机之间可以互相访问. 而攻击者的意图是窃取目标主机 IP5 上的信息.

3.2　实验结果与分析

在没有估价函数的情况下进行盲目搜索,生成了完整的攻击图,攻击图有 106 个节点和 105 条边,到达攻击目标的攻击路径有 46 条. 由于生成攻击图的时间长,规模大,网络管理员无法从复杂的攻击图中快速有效的获得有价值信息. 接着,采用本文设计的算法,产生的攻击图如图 2.

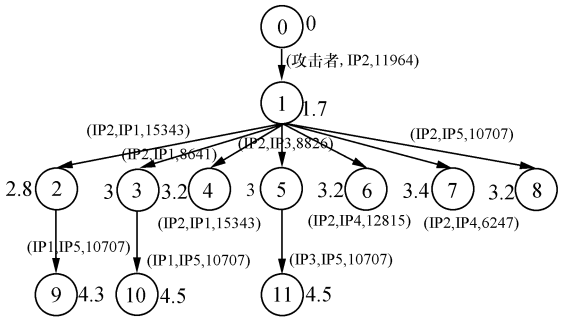

图 2　基于有序搜索生成的攻击图

Fig. 2　The attack graph based on sequential search generation algorithm

图 2 中状态节点旁边的数字代表当前节点的估价函数值. 图中共有 12 个节点和 11 条边,可以看出,通过有序搜索攻击图生成算法,生成攻击图的规模较小. 从生成的攻击图可以发现,攻击者攻击 IP2 主机的 11964 弱点,攻取 IP2 的 Root 权限后,通过 IP2 攻击 IP5 的 10707 弱点而成功获取 IP5 的 Root 权限,这条路径的攻击代价最小,攻击者一般会最优先选择该路径攻击,因此网络管理员应该重点提防.

4　结　论

网络安全研究在信息社会中具有重要的意义,也是一项有挑战性的工作. 本文采用有序搜索,基于估价函数值作为网络状态节点扩展的依据,降低了攻击图生成的时间复杂性,有效控制了生成攻击图的规模. 仿真实验证明算法的可行性和有效性,为网络管理员管理网络决策与防范提供指导帮助.

参考文献:

[1] Zhang L, Tang H, Cui Y, et al. Network security evaluation through attack graph generation[J]. World Academy of Science, Engineering and Technology, 2009, 54(1): 412-416.

[2] Khaitan S, Raheja S. Finding optimal attack path using attack graphs: a survey[J]. International Journal of Soft Computing and Engineering, 2011, 1(3): 33-36.

[3] Chen F, Liu D, Zhang Y, et al. A scalable approach to analyzing network security using compact attack graphs [J]. Journal of Networks, 2010, 5(5): 543-550.

[4] Wang C, Du N, Yang H. Generation and analysis of attack graphs[J]. Procedia Engineering, 2012, 29: 4053-4057.

[5] Liu Z, Li S, He J, et al. Complex network security analysis based on attack graph model[C]//Sun S, Guo S, Yu F, et

al. Second International Conference on Instrumentation, Measurement, Computer, Communication and Control (IMCCC), 2012. Los Alamitos: IEEE, 2012: 183-186.

[6] Phillips C, Swiler L P. A graph-based system for network-vulnerability analysis[C]//Bob Blakeley, Darrell Kienzle, Mary Ellen Zurko. Proceedings of the 1998 workshop on New security paradigms. New York: ACM, 1998: 71-79.

[7] Swiler L P, Phillips C, Ellis D, et al. Computer-attack graph generation tool[C]//Frances M. Titsworth. DARPA Information Survivability Conference & Exposition II, 2001. DISCEX 01. Proceedings. Los Alamitos: IEEE, 2001, 2: 307-321.

[8] Ritchey R W, Ammann P. Using model checking to analyze network vulnerabilities[C]//Frances M. Titsworth. Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. Los Alamitos: IEEE, 2000: 156-165.

[9] Sheyner O, Haines J, Jha S, et al. Automated generation and analysis of attack graphs[C]//A. Denise Williams. Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on. Los Alamitos: IEEE, 2002: 273-284.

[10] Sheyner O M. Scenario graphs and attack graphs[D]. Madison: University of Wisconsin, 2004.

[11] Ammann P, Wijesekera D, Kaushik S. Scalable, graph-based network vulnerability analysis[C]//Vijay Atluri. Proceedings of the 9th ACM Conference on Computer and Communications Security. New York: ACM, 2002: 217-224.

[12] Noel S, Jajodia S. Managing attack graph complexity through visual hierarchical aggregation[C]//Carla Brodley, Philip Chan. Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security. New York: ACM, 2004: 109-118.

[13] Noel S, Jacobs M, Kalapa P, et al. Multiple coordinated views for network attack graphs[C]//Kwan-Liu Ma, Stephen C. North, William Yurcik: IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05). Los Alamitos: IEEE, 2005: 99-106.

[14] Li W, Vaughn R B. Cluster security research involving the modeling of network exploitations using exploitation graphs[C]//Stephen John, Bu Sung Lee, Cai W. Sixth IEEE International Symposium on Cluster Computing and the Grid, 2006 (CCGRID 06). Los Alamitos: IEEE, 2006: 26-26.

[15] Dawjubs J, Wale J. A systematic approach to multi-stage network attack analysis[C]//Jack Cole, Zheng Y. Proceedings of the Second IEEE International Information Assurance Workshop (IWIA04). Los Alamitos: IEEE, 2004: 48-54.

[16] 苘大鹏,周渊,杨武,等. 用于评估网络整体安全性的攻击图生成方法[J]. 通信学报,2009,30(3):1-5.

[17] 苘大鹏,张冰,周渊,等. 一种深度优先的攻击图生成方法[J]. 吉林大学学报(工学版),2009,39(2):446-452.

[18] 吴淑语,李波. 基于攻击模式的广度搜索攻击图生成算法[J]. 重庆工商大学学报(自然科学版),2012,29(12):44-48.

[19] 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.

[20] Man D, Zhang B, Yang W, et al. A method for global attack graph generation[C]//Liu D, Chai T, Wang J. 2008 IEEE International Conference on Networking, Sensing and Control (ICNSC 2008). Los Alamitos: IEEE, 2008: 236-241.

[21] Xie A, Zhang L, Hu J, et al. A probability-based approach to attack graphs generation[C]//Li M, Yu F, Shu J, et al. Second International Symposium on Electronic Commerce and Security, 2009 (ISECS 09). Los Alamitos: IEEE, 2009: 343-347.

[22] 蔡自兴,徐光祐. 人工智能及其应用[M]. 4 版. 北京:清华大学出版社,2010.

[23] 苘大鹏,杨武,杨永田. 基于攻击图的网络脆弱性分析方法[J]. 南京理工大学学报:自然科学版,2008,32(4):416-419.

[24] 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.